KEEPING AMERICA SECURE: THE SCIENCE SUPPORTING THE DEVELOPMENT OF THREAT DETECTION TECHNOLOGIES

HEARING

BEFORE THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

THURSDAY, JULY 19, 2012

Serial No. 112–97

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PRINTING OFFICE

75–393PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. RALPH M. HALL, Texas, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
ROSCOE G. BARTLETT, Maryland
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
PAUL C. BROUN, Georgia
SANDY ADAMS, Florida
BENJAMIN QUAYLE, Arizona
CHARLES J. "CHUCK" FLEISCHMANN, Tennessee
E. SCOTT RIGELL, Virginia
STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
ANDY HARRIS, Maryland
RANDY HULTGREN, Illinois
CHIP CRAVAACK, Minnesota
LARRY BUCSHON, Indiana
DAN BENISHEK, Michigan
VACANCY

EDDIE BERNICE JOHNSON, Texas
JERRY F. COSTELLO, Illinois
LYNN C. WOOLSEY, California
ZOE LOFGREN, California
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
JERRY McNERNEY, California
TERRI A. SEWELL, Alabama
FREDERICA S. WILSON, Florida
HANSEN CLARKE, Michigan
SUZANNE BONAMICI, Oregon
VACANCY
VACANCY
VACANCY

CONTENTS

Thursday, July 19, 2012

KEEPING AMERICA SECURE: THE SCIENCE SUPPORTING THE DEVELOPMENT OF THREAT DETECTION TECHNOLOGIES

THURSDAY, JULY 19, 2012

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Committee met, pursuant to call, at 10:04 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Ralph Hall [Chairman of the Committee] presiding.

RALPH M. HALL, TEXAS
CHAIRMAN

EDDIE BERNICE JOHNSON, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

Subcommittee On Space and Aeronautics

Spurring Economic Growth and Competitiveness Through NASA Derived Technologies

Thursday, July 12, 2012
10:00 a.m.-12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Dr. Mason Peck, NASA Chief Technologist
Mr. George Beck, Chief Clinical and Technology Officer, Impact Instrumentation, Inc.
Mr. Brian Russell, Chief Executive Officer, Zephyr Technology
Mr. John Vilja, Vice President for Strategy, Innovation and Growth, Pratt & Whitney Rocketdyne
Dr. Richard Aubrecht, Vice President, Moog, Inc.

SUBCOMMITTEE ON SPACE AND AERONAUTICS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

Spurring Economic Growth and Competitiveness Through NASA Derived Technologies

Thursday, July 12, 2012

10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

NASA is often considered an incubator for technology development, and history has shown a vast array of technologies that owe their start to NASA programs. Despite decades of demonstrated success, federal investment in NASA remains essentially flat even as other R&D agencies are seeing increases. Furthermore, investment in NASA's technology transfer activities has seen a drastic decline in recent years.

The purpose of this hearing will be to examine the direct economic and societal benefits that investments in NASA have generated and highlight those areas where continued investments could help stimulate the pipeline for future economic growth.

Witnesses

- **Dr. Mason Peck,** NASA Chief Technologist
- **Mr. George Beck,** Chief Clinical and Technology Officer, Impact Instrumentation, Inc.
- **Mr. Brian Russell,** Chief Executive Officer, Zephyr Technology
- **Mr. John Vilja,** Vice President for Strategy, Innovation and Growth, Pratt & Whitney Rocketdyne
- **Dr. Richard Aubrecht,** Vice President, Moog, Inc.

Background

The National Aeronautics and Space Act of 1958 established NASA as the leading agency for aeronautical and space sciences, and specifically directed that the new agency would "provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof."[1] Since then, NASA has developed innovative technologies that are ubiquitous to daily civilian and military life in the United States – and even the world. Besides

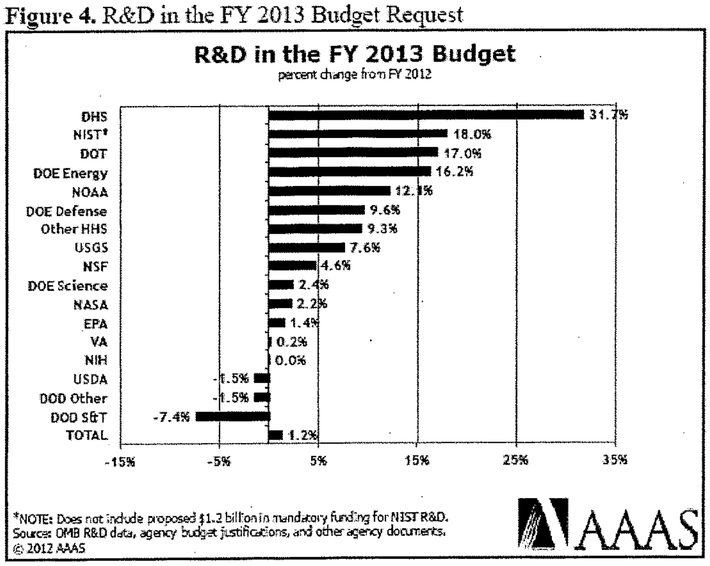
[1] http://history.nasa.gov/spaceact.html

being the global leader in advanced aircraft and spacecraft design, NASA technologies have paved the way for advances in the medical field, environmental stewardship, and public safety.

The Stevenson-Wydler Technology Innovation Act of 1980 and the Federal Technology Transfer Act of 1986 also support NASA's technology transfer activities. Each mandate the promotion of federally-funded research and technology transfer to the commercial sectors, and state and local governments. They also grant authority to Government-owned and Government-operated laboratories to enter into cooperative research and development agreements with the private sector and with academia.

On October 28, 2011, President Obama issued a memorandum entitled, "*Accelerating Technology Transfer and Commercialization of Federal Research in Support of High Growth Businesses*," requiring all Federal agencies to identify opportunities for, and plan transitions to, increase the number of technology transfer and commercialization activities.[2] As the chart below demonstrates, however, funding for research and development at NASA is barely keeping pace with inflation – even as other agencies are reaping the benefits of increased investments.

Figure 4. R&D in the FY 2013 Budget Request



[3]

[2] http://www.whitehouse.gov/the-press-office/2011/10/28/presidential-memorandum-accelerating-technology-transfer-and-commerciali

[3] AAAS Report, Federal Research &Development FY 2013, p. 14

It should be noted that the FY 2013 budget request for the Space Technology Directorate was $699 million, an increase of $125.3 million. The SBIR and STTR programs are required by federal law to represent a base percentage of R&D (currently 2.7% for FY 2013). The Partnership Development and Strategic Integration Program – central to carrying out the agency's technology transfer and commercialization efforts – would receive only $29.5 million.

	Actual	Estimate		Notional			
Budget Authority (in $ millions)	**FY 2011**	**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**	**FY 2016**	**FY 2017**
FY 2013 President's Budget Request	456.3	573.7	699.0	699.0	699.0	699.0	699.0
SBIR and STTR	164.7	166.7	173.7	181.9	187.2	195.3	206.0
Partnerships Dev & Strategic Integration	25.6	29.5	29.5	29.5	29.5	29.5	29.5
Crosscutting Space Tech Development	120.4	187.7	293.8	272.1	266.6	259.7	247.0
Exploration Technology Development	144.6	189.9	202.0	215.5	215.7	214.5	216.5

Office of Chief Technologist

The Office of Chief Technologist (OCT) manages NASA's Space Technology programs and coordinates and tracks all technology investments across the agency. The office is also the primary point of contact with other government agencies and outside entities and is responsible for managing innovative technology partnerships, technology transfer and commercial activities. There are four programs that support the transfer of technology:

- The Small Business Innovative Research (SBIR) and Small Business Technology Transfer (STTR) Programs – which apply to all federal departments and agencies - were established by Congress in 1982 to aid small and disadvantaged businesses to partner with federally funded research and development programs.
- The Crosscutting Space Technology Development Program focuses on developing capabilities that advance future space missions.
- The Exploration Technology Development Program focuses on advancing the development of technologies to enable human missions.
- The Partnership Development and Strategic Integration Program provides for the transfer and commercialization of NASA-developed technologies, coordinates interagency technologies, and manages intellectual property rights. This program also seeks out opportunities for partnership with other government agencies and industry.

While the first three of these programs seek to identify and develop technologies specifically to meet agency mission objectives, the fourth program seeks to push NASA-derived technology out into the private sector. The Innovative Partnerships Office (IPO), part of the Partnership Development and Strategic Integration Program, seeks to promote innovative partnership opportunities to commercialize technology that can be transferred from NASA's programs and projects. Each NASA Center also has an IPO and a Chief Technologist that work directly with OCT.

It should be noted that the SBIR/STTR programs – while focusing on technologies that can be infused into NASA's missions – have consistently yielded spinoff technologies into the private sector. As a result, approximately 30% of all spinoff technologies reported by NASA over the last decade can be attributed to SBIR/STTR partnerships.

NASA Inspector General Report on Technology Transfer

In March 2012, the NASA Inspector General issued an *Audit of NASA's Process for Transferring Technology to the Government and Private Sector.* The report concluded:

> NASA has missed opportunities to transfer technologies from its research and development efforts and to maximize partnerships that could provide additional resources, and industry and the public have not fully benefited from NASA-developed technologies.[4]

For example, the primary tracking mechanism for reporting potentially transferrable technologies is through New Technology Reports (NTRs). NTRs are submitted by NASA employees and contractors who develop new technologies and are reviewed by the IPO and Patent Counsel to determine their technical merit. But as the table below highlights, NASA's ability to adequately process NTRs and consequently move promising technologies forward has been declining. The table notes that despite having over 1,800 NTRs filed in FY 2011, the number of patents filed was only 82 (contrasted to FY 2004 when only 585 NTRs were submitted yielding 131 filed patents).

Table 3. NASA NTR and Patent Filing Status at the End of Each Fiscal Year and Fiscal Year Technology Transfer Funding Levels

Fiscal Year	Cumulative NTRs under Evaluation	Cumulative NTRs Awaiting/ Preparing Patent Application	Patent Application under Prosecution	Patent Filed	Technology Transfer Funding (million)
2004	585	6	20	131	$60.00
2005	654	6	28	135	$45.30
2006	725	7	41	127	$38.25
2007	844	11	81	109	$26.60
2008	1,017	14	140	117	$38.10
2009	1,493	26	322	115	$23.60
2010	1,504	30	296	98	$20.54
2011	1,878	34	372	82	$20.54

[4] *Audit of NASA's Process for Transferring Technology to the Government and Private Sector,* IG Report No. IG-12-013, March 1, 2012, p. iv

As demonstrated above, the percentage of NASA's overall budget for technology transfer funding has steadily declined. According to the NASA IG:

> Since fiscal year 2004, funding for NASA's technology transfer efforts has decreased by 68 percent, from $60 million in 2004 to $19.2 million in FY2012 [from within the Partnership Development and Strategic Integration funding line]. In addition, personnel resources dedicated to the technology transfer effort have similarly declined. For example, since FY 2003 the number of patent attorneys at the Centers has dropped from 29 to 19 and Headquarters IPO staff has decreased from 13 in FY 2010 to just 2 in FY 2012.[5]

The IG provided recommendations to the NASA Chief Technologist to improve NASA's technology transfer and commercial efforts. Specifically, the Chief Technologist should:

- Implement procedures to ensure appropriate personnel are held accountable to the [NASA] requirements
- Provide relevant periodic training to NASA personnel
- Reassess the allocation of resources for technology transfer
- Coordinate with the Chief Engineer to ensure NASA Policy Requirements emphasized the importance of developing Commercialization Plans
- Coordinate with the General Counsel to ensure NTRs are accessible to NASA project managers and innovators as appropriate

The Chief Technologist concurred with the IG recommendations and is currently undergoing evaluations and implementing changes to improve the policies governing technology transfer and the training necessary to ensure Agency employees and contractors are following procedures to maximize effectiveness.

NASA Spinoffs

NASA defines a spinoff as "a commercially available product, service or process that takes NASA-related technology and brings it to a broader audience."[6]

Since 1976, NASA has documented successful examples of technology transfer and commercialization in its annual *Spinoffs* publication. Over 1,750 case studies have demonstrated the tremendous economic and societal benefits that have been generated in fields as diverse as computer technology, manufacturing, health and medicine, public safety, consumer goods, and energy conversion and use.

Examples from the most recent publication, *Spinoffs 2011* include:

- ***Impact Instrumentation, Inc., West Caldwell, New Jersey***. Drawing on the expertise of Johnson Space Center space medicine experts under the auspices of a Space Act Agreement, Impact Instrumentation Inc. made advances in medical ventilator technology

[5] IG Report No. IG-12-013, March 1, 2012, p. iii
[6] *Spinoff 2010*, Forward, p. 7

now incorporated into emergency medical solutions for soldiers and civilians around the world.

- ***Zephyr Technology, Annapolis, Maryland:*** Through a Space Act Agreement with *Ames Research Center*, Zephyr Technology worked with NASA physiology experts on motion sickness experiments, resulting in improvements to the company's wearable vital-sign monitors. Zephyr's monitors are now used to monitor the health and fitness of soldiers, first responders, pro athletes, and average consumers looking to get in shape. The company sells thousands of its U.S. manufactured NASA-enhanced products each month.
- ***Pratt & Whitney Rocketdyne, Canoga Park, California***: The Space Shuttle Main Engine was designed under contract to NASA by Rocketdyne, now part of Pratt & Whitney Rocketdyne (PWR). After working with *Marshall Space Flight Center*, PWR used its rocket engine experience to make clean energy gasification technology with 10-20 percent lower capital costs and a 10-percent reduction in carbon dioxide emissions, compared to conventional technology.

NASA's Technology Commercialization Policy

NASA has established formal procedural requirements for technology commercialization. Accordingly, NASA project managers must consider commercialization potential early in the project's life cycle and, where appropriate, develop a Technology Commercialization Plan and strategy for achieving that potential. The policy outlines considerations for the commercialization plan, including pursuing partnerships, cooperative agreements and Space Act Agreements. In addition, the policy requires that new technologies and inventions and resulting success stories must be reported.

The policy provides specific and detailed guidance to NASA program and project managers related to formulating, approving, implementing, and evaluating their technology commercialization activities. Specifically, "NASA managers are challenged to use their expertise and apply innovative techniques to ensure that the technological assets (technologies, innovations, facilities and expertise) from their activities have maximum commercial application."[7]

[7]NASA Procedural Requirements 7500.1, "NASA Technology Commercialization Process w/Change 1 (4/9/04)" http://nodis3.gsfc.nasa.gov/npg_img/N_PR_7500_0001_/N_PR_7500_0001_.pdf, p. 9-10

Chairman HALL. The Committee on Science, Space, and Technology will come to order, and I say to you, good morning and thank you. Welcome to today's hearing entitled "Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies."

In front of you are packets containing the written testimony for all of the Members that are here, biographies and Truth in Testimony disclosures for today's witnesses. I will recognize myself for five minutes for an opening statement. I once again welcome everybody to the hearing.

The September 11th terrorist attacks forced the American public to confront the daily threat of domestic terrorism, and advancing threat detection technologies, I think, is one of the many ways research and development contributes to keeping our country secure. Recognizing the need to respond quickly when a potential threat is identified and to counter the growing list of threats to our country, the U.S. government and the private sector focused research and development activities on the detection of explosives, firearms, and dangerous materials including chemical, biological, radiological, and nuclear matter. Scientific research has advanced the development of technologies to protect the Nation, but the rapidly changing threats that we face require continued research and development to ensure that we keep ahead of our enemies. We recognize that the terrorists only need to get it right once to succeed, whereas we need to get it right every time to ensure the protection of our citizens.

I think that with highly visible events such as the Olympic Games and the Democratic and Republican National Conventions occurring this summer, and major sporting events that you all are well aware of more so than probably some of us, and because of your duties and requirements and your knowledge, and major sporting events and concerts are drawing crowds of thousands on a weekly basis, there is continued interest in improving existing threat detection technologies and advancing new ones.

Today, we have the opportunity to examine some of the research and development activities that the Federal Government is undertaking to support the advancement of threat detection technology. The research and development activities occurring at these federal agencies that we have talked about have the potential to both transform and improve threat detection, and to create products and technologies that could be beneficial for other purposes.

While I recognize that threat detection is only one piece of a much larger system required to combat terrorism, better detection does enable better protection for our citizens. As the old saying goes, an ounce of prevention is worth a pound of cure.

I look forward to hearing more about the ongoing research designed to improve physical threat detection, protect the public, and support the development of marketable technologies.

And I certainly thank our witnesses for your time, the time it took you to prepare to come here, the time in your life that prepared you to be at that table. You are the ones who write the legislation that we pass, and we thank you for your time and thank you for your appearance here today and your willingness to testify before us.

I yield back my time.

[The prepared statement of Mr. Hall follows:]

PREPARED STATEMENT OF CHAIRMAN RALPH HALL

Good Morning. I would like to welcome everyone to today's hearing.

The September 11th terrorist attacks forced the American public to confront the daily threat of domestic terrorism. Advancing threat detection technologies is one of the many ways research and development contributes to keeping America secure. Recognizing the need to respond quickly when a potential threat is identified and to counter the growing list of threats to our country, the U.S. government and the private sector focused research and development activities on the detection of explosives, firearms, and dangerous materials including chemical, biological, radiological, and nuclear matter. Scientific research has advanced the development of technologies to protect the Nation, but the rapidly changing threats that we face require continued research and development to ensure that we keep ahead of our enemies. We recognize that the terrorists only need to get it right once to succeed, whereas we need to get it right every time to ensure the protection of our citizens.

In March of this year a Gallup poll[1] showed that terrorism ranked near the bottom of fifteen issues facing the country today–behind the economy, gas prices, unemployment, drug use, and the environment, among others. This may be partly because of the success we have had in protecting the Nation since 9/11. Economic issues dominate day-to-day concerns right now, so it is easy to become complacent about the threat of terrorism. However, with highly visible events such as the Olympic Games and the Democratic and Republican National Conventions occurring this summer, and major sporting events and concerts drawing crowds of thousands on a weekly basis, there is continued interest in improving existing threat detection technologies and advancing new ones.

Today, we have the opportunity to examine some of the research and development activities that the Federal government is undertaking to support the advancement of threat detection technologies. The National Institute of Standards and Technology, the Domestic Nuclear Detection Office, the National Science Foundation, and the Pacific Northwest National Laboratory are all investigating different aspects of threat detection.

The research and development activities occurring at these federal agencies have the potential to both transform and improve threat detection, and to create products and technologies that could be beneficial for other purposes, such as nuclear applications for use in medicine.

While I recognize that threat detection is only one piece of a much larger system required to combat terrorism, better detection does enable better protection for our citizens. As the old saying goes, an ounce of prevention is worth a pound of cure.

I look forward to hearing more about the ongoing research designed to improve physical threat detection, protect the public, and support the development of marketable technologies.

Thank you to our witnesses for your willingness to testify before us today.

I yield back my time.

Chairman HALL. I recognize Mrs. Johnson for an opening statement.

Ms. JOHNSON. Thank you very much, Mr. Hall, and thank you for calling this hearing to examine terrorist threat detection technologies. Unfortunately, we live in a world where terrorist threats are growing and we have to be prepared to detect and respond to these threats.

I also want to thank our witnesses for being here today. We certainly appreciate all that you are doing to advance threat detection technology and to keep us safe from those who seek to do us harm. Without a doubt, there is a lot of good work going on in these areas and you all should be commended for the part that you play in that.

---

[1] http://www.gallup.com/poll/153485/Economic-Issues-Dominate-Americans-National-Worries.aspx

There is no denying, of course, that this sort of good work costs money. We are all so painfully aware that in recent years, federal budgets have been tight and that funding has been constrained. I am interested in hearing today about how reduced or stagnant funding levels have hampered or challenged your terrorist threat detection activities, if at all. Sometimes with a little tighter belt, you can produce better work. We will see. I am also interested in learning what steps your agencies are taking to leverage the limited resources available for these activities, and I am curious about how your threat detection research is prioritized, not only within your individual agencies, but across the Federal Government. I would also like to learn more about how you are partnering with non-federal entities to ensure that the most promising and most impactful research is still being conducted and does not fall victim to the budget wars we are waging here in Congress.

I have had the opportunity to review your written testimony and am impressed by the technologies that have been developed in recent years. However, for our purposes today, I am most interested in learning about the challenges that remain, where we ought to be making future investments, and what this Committee can do to ensure that the new research is supported. The truth is that we must stay at least one step ahead of the terrorists and our threat detection research is our first line of defense.

I also understand that there are challenges to deterring terrorist threats that go beyond mere detection. We can have the best threat protection technologies imaginable, but our ability to thwart a terrorist attack rests on our capability to interpret that threat and respond to it. I am interested in hearing about what is being done throughout the Federal Government to ensure that we respond appropriately when a threat is detected and how, if at all, your agencies are feeding into that process.

And finally, we cannot ignore the very important role that social and behavioral sciences play in helping to keep us safe from terrorist attacks. We need to understand more than just the bomb or how to detect the bomb. We also need to understand the bomb maker. We need to understand not only what motivates someone to make or use that bomb, but also what specific groups and which specific individuals are most likely to make and attack us with that bomb. There is important social and behavioral science work going on in this area, including at the Department of Homeland Security's Science and Technology Directorate, at the National Science Foundation, and through the federally supported National Consortium for the Study of Terrorism and Responses to Terrorism, and I hope that we will have an opportunity to touch on this important research today.

Again, Mr. Chairman, I thank you for holding the hearing and I yield back the balance of my time.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF RANKING MEMBER EDDIE BERNICE JOHNSON

Thank you, Chairman Hall, for calling this hearing to examine terrorist threat detection technologies. Unfortunately, we live in a world where terrorist threats are growing and we have to be prepared to detect and respond to these threats.

I also want to thank our witnesses for being here today. We certainly appreciate all that you are doing to advance threat detection technology and to keep us safe from those who seek to do us harm. Without a doubt, there is a lot of good work going on in this area and you all should be commended for your part in that.

There is no denying, of course, that this sort of good work costs money. We are all painfully aware that, in recent years, Federal budgets have been tight and that funding has been constrained. I am interested in hearing today about how reduced or stagnant funding levels have hampered your terrorist threat detection activities, if at all.

I am also interested in learning what steps your agencies are taking to leverage the limited resources available to you for these activities. I am curious about how your threat detection research is prioritized—not only within your individual agency, but also across the Federal Government. I would also like to learn more about how you are partnering with non-Federal entities to ensure that the most promising and most impactful research is still being conducted and does not fall victim to the budget wars we are waging here in Congress.

I have had the opportunity to review your written testimony and am impressed by the technologies that have been developed in recent years. However, for our purposes today, I am most interested in learning about the challenges that remain, where we ought to be making future investments, and what this Committee can do to ensure that this new research is supported. The truth is that we must stay at least one step ahead of the terrorists and our threat detection research is our first line of defense.

I also understand that there are challenges to deterring terrorist threats that go beyond mere detection. We can have the best threat detection technologies imaginable, but our ability to thwart a terrorist attack rests on our capacity to interpret that threat and respond to it. I am interested in hearing about what is being done throughout the Federal Government to ensure that we respond appropriately when a threat is detected and how, if at all, your agencies are feeding into that process.

Finally, we cannot ignore the very important role that social and behavioral sciences play in helping to keep us safe from terrorist attacks.

We need to understand more than just the bomb or how to detect the bomb. We also need to understand the bomb maker. We need to understand not only what motivates someone to make or use that bomb, but also what specific groups and which specific individuals are most likely to make and attack us with that bomb. There is important social and behavioral science work going on in this area, including at the Department of Homeland Security's Science and Technology Directorate, at the National Science Foundation, and through the federally-supported National Consortium for the Study of Terrorism and Responses to Terrorism. I hope that we will have an opportunity to touch on this important research today.

Chairman HALL. And I thank you, and I thank you for the warnings. As a matter of fact, in Bulgaria just yesterday, I am told that Israeli citizens were attacked and seven killed and about 30 injured, so we have these things to read about, hear about and be warned about. I think our hearing is very timely, and I thank you for yielding back.

If there are Members who wish to submit additional opening statements, your statements can be added to the record at this time or before we complete our hearing today.

Now I would like to introduce our panel of witnesses. I have already thanked you, and I will do that again. Our first witness is Dr. Richard Cavanagh, the Director of the Office of Special Programs at the National Institute of Standards and Technology. Dr. Cavanagh is responsible for measurement science and standards in biology, chemistry and material science.

Our second witness is Dr. Huban Gowadia, the Acting Director for the Domestic Nuclear Detection Office at the Office of Homeland Security. In this role, Dr. Gowadia oversees integration of interagency efforts for technical and nuclear detection and forensics. In addition, she directs the Department's radiological and nuclear detection capabilities.

Our next witness is Dr. Anthony Peurrung, the Associate Laboratory Director for the National Security Directorate at the Pacific

Northwest National Laboratory. Dr. Peurrung has been with the National Security Directorate since 1994 during which time he has done research on a variety of topics including special nuclear material detection.

Our final witness for today is Dr. Thomas Peterson, the Assistant Director for the Directorate for Engineering at the National Science Foundation. Dr. Peterson helps guide the Directorate in its mission of supporting fundamental and transformative research that enhances the competitiveness of the United States.

As our witnesses know, spoken testimony is limited to five minutes but we appreciate you so much and thank you so much, we are not going to hold you to that. Just do your best, and whatever you do, you will not be gaveled down. Nobody has a hook that will reach for or anything. Just help us because we need you and we appreciate you.

I now recognize the witnesses to present their testimony. Dr. Cavanagh, you are recognized for five minutes to present your testimony, sir.

STATEMENT OF DR. RICHARD CAVANAGH, DIRECTOR, OFFICE OF SPECIAL PROGRAMS, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. CAVANAGH. Chairman Hall, Ranking Member Johnson and Members of the Committee, thank you for the opportunity to appear before you today to discuss the important role that the Department of Commerce's National Institute of Standards and Technology, NIST, plays in threat detection technologies. Today we are driven to detect and respond to threats in ways that are faster, more definitive and rely on multiple detection technologies.

As new threats emerge, new detection techniques are often needed to ensure the safety of the American public. It is in this mission space that NIST works to support industry and other federal agencies in meeting these measurement and standards challenges.

My testimony will today highlight NIST's role and give examples of NIST's work where the application of our measurement and standards expertise has helped assure the quality and reliability and advance the state-of-the-art detection methods used to protect the Nation.

NIST is responsible for developing and validating measurement methods and standards that will allow industry to accurately and reproducibly assess their processes and products. So when the Department of Homeland Security needed to facilitate manufacturer-independent transfer of information from radiation measurement instruments for use in homeland security applications, as well as for detection of illicit trafficking of radioactive materials, they called on NIST, and a test and evaluation program for detection equipment was established.

NIST is also working with DHS in the development of standards to address the mandate in the SAFE Port Act to protect our ports from chemical, biological, nuclear and explosive threats. To this end, NIST has applied its experience in the development of calibration standards and measurements to help DHS and private-sector standards organizations develop a test and evaluation program to measure and characterize the sensitivity of portal monitors that are used to scan shipping containers for radiation and nuclear threats.

NIST works closely with agencies such as DHS, DOD and DOJ, which are responsible for anticipating emerging threats to remain attuned to the threats that are on the horizon and develop appropriate measurement assurance plans in collaboration with those lead agencies. An example of this kind of interaction can be seen in the recently released *National Strategy for Chemical, Biological, Radiological, Nuclear and Explosive Standards* that was jointly developed with DHS, EPA and NIST. In addition, NIST is currently working with DHS to develop common test methods for chemical, biological, radiological and nuclear commercial off-the-shelf equipment. This effort will avoid duplication in testing efforts across several government agencies.

To protect travelers, NIST has worked on standards for swipe sampling for trace explosives. An example of this method is deployed in airports where objects are swiped with a cloth that is then quickly analyzed. Working with DHS, NIST has developed standard methods for swipe sampling for biologics such as suspicious white powders and for trace explosives. These methods have been dramatically improved through developments in measurement science.

NIST continues to make advances in this space, and we are currently working on solving the measurement challenges that must be overcome to incorporate trace explosive detection methods into card readers and to assist local, state and federal agencies in the detection and response to chemical and biological threats.

In the wake of the anthrax attacks, the first-responder community needed better guidance and protocols to enable effective detection of biothreat agents during response and decontamination operations. Working with DHS and standards organizations, NIST led the effort to develop the standard for the collection of suspected biological threat agents and for the initial response to suspected threats. Work at NIST is also being done in the development of systems to detect trace amounts of chemicals or toxins in air and water.

Standards are important in quantifying the level of confidence that can be placed in any data. NIST's focus is on the measurements. With deep expertise in dealing with measurement repeatability and uncertainty in such wide-ranging areas as chemical, nuclear, biological and explosives, we are well positioned to support the measurement assurance needs of academia, industry and other federal agencies. We do this through development of standards, guidance, calibrations and reference materials and by providing technical advice when and where needed.

In conclusion, NIST expertise in measurement science and standards is playing a recognized role in providing the country with robust threat detection capabilities.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

[The prepared statement of Dr. Cavanagh follows:]

Testimony of

Dr. Richard R. Cavanagh
Director Office of Special Programs
National Institute of Standards and Technology
Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space, and Technology

Keeping America Secure:
The Science Supporting the Development of Threat Detection Technologies

July 19, 2012

Chairman Hall, Ranking Member Johnson, and Members of the Committee, thank you for the opportunity to appear before you today to discuss the important role that the National Institute of Standards and Technology (NIST) plays in threat detection technologies. Industry, Public Safety, Security, and Defense are all driven to detect and respond to threats in ways that are faster, more definitive, and rely on multiple detection technologies.

Detection technologies are becoming less intrusive, faster, and more sensitive with fewer false signals. As new threats emerge, new detection are often needed to ensure the safety of the American public. Novel detection techniques typically require new measurement standards to validate their operation, to assure that they are reliable and appropriately sensitive.

It is in this mission space that the Department of Commerce's NIST works to support industry and other Federal agencies in meeting these measurement and standards challenges. My testimony today will highlight NIST's role and give examples of NIST's work where the application of our measurement and standards expertise has helped assure the quality and reliability and advanced the state of the art of detection methods used to protect the nation.

NIST's Role in Research and Development in Threat Detection Technology

NIST was established with a specific mission -- to define and advance a uniform, scientific, national system of measurement to support industry and other federal agencies. This system of measurement is underpinned by NIST's measurement science research.

In that role, NIST is responsible for developing and validating measurement methods and standards that will allow industry to accurately and reproducibly assess their processes and products, including the presence of hazardous chemicals in a manufacturing process, monitoring the growth of biopharmaceuticals, and calibration of detectors used to assure that safe doses are delivered in medical treatments like radiation oncology.

The research infrastructure required to enable reliable and reproducible measurements in these important sectors of our economy is frequently well aligned with the research infrastructure which is required to support the accurate and reproducible detection of chemical agents, biological threats, radiological and nuclear threats.

Well defined measurement standards are central when comparing different technologies that are aimed at detecting the same threat in different scenarios, when comparing detection sensitivities of different measurement technologies, and when comparing data obtained by detectors used by Military versus Civilian agencies.

So when the Department of Homeland Security (DHS) Domestic Nuclear Detection Office (DNDO) needed to facilitate manufacturer-independent transfer of information from radiation measurement instruments for use in homeland security applications as well as for detection of illicit trafficking of radioactive materials, they talked to NIST. Working with the American National Standards Institute (ANSI) and the Institute of Electrical and Electronics Engineers (IEEE), a test and evaluation program for detection equipment was established. The data are currently maintained by NIST as part of the program. NIST is also working with DNDO in the development of Technical Capability Standards to address the mandate in the SAFE Port Act (PL 109-347) to protect our ports from chemical, biological, nuclear and explosive (CBRNE) threats. NIST participates with the DHS Science and Technology Directorate (S&T) in the development of standards for devices which detect chemical and biological agents.

Partnering with Other Government Agencies, Industry, and Academia to Leverage Efforts and Avoid Duplication

NIST works closely with agencies such as the Department of Homeland Security (DHS), the Department of Defense (DOD), the Department of Justice (DOJ), and the National Nuclear Security Administration (NNSA), which are responsible for anticipating emerging threats. Through interactions with their program managers, mission leads, and interagency working groups, NIST is able to remain attuned to threats that are on the horizon, and develop appropriate measurement assurance plans in collaboration with the lead agencies. An example of this kind of interaction can be seen in the recently released National Strategy for Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Standards that was jointly developed by DHS, the Environmental Protection Agency (EPA) and NIST.

NIST helps other federal agencies understand both the scientific basis for potential detection technologies for these emerging threats, and the developments that would be required to achieve a robust and reliable measurement protocol. Given our primary mission to support industry, we are frequently in a position to point to existing detection technology that could be appropriate for detection of an emerging threat. NIST is also in a position to develop measurement standards that meet the need of both industry and the government agencies.

As an example of our support to other government agencies, NIST has been able to apply its experience in the development of calibration standards and measurements used to determine the radiation doses received in various medical procedures in treatments (e.g., mammography, brachytherapy) to help DHS develop methodologies that will measure and characterize the sensitivity of portal monitors that are used to scan shipping containers for radiation and nuclear threats.

NIST is currently working with DHS, and specifically DNDO, S&T, and the Office of Health Affairs, and also with DOD to develop common test methods and testing capabilities for Chemical, Biological, Radiological and Nuclear commercial off the shelf equipment. This effort will avoid duplication in testing efforts across several government agencies. As part of this effort the National Voluntary Laboratory Accreditation Program (NVLAP) is being used for the accreditation of the testing laboratories that are involved in the radiological and nuclear detection tests.

NIST also interacts with academia and industry through standards development organizations, workshops and conferences to ensure transparency of our efforts, and to stay abreast of emerging detector capabilities.

In particular, NIST looks to areas in which the absence of validated data is limiting the utility of a method, where research in measurement methods is required to establish that a method is suited for reliable use in the field, and where the lack of reference material or calibration is a roadblock to technical progress. Frequently, we get an understanding of new measurement needs through engagement with thought leaders in academia who are delving into the frontiers of science.

Successes and Current Challenges of Improved Detection

Swipe Sampling and Trace Explosives — The best example of this method is deployed in airports where persons or objects are swiped with a cloth that is then quickly analyzed. Working with DHS and the Transportation Security Administration (TSA), NIST has helped develop standard methods for swipe sampling for biologics such as suspicious white powders and for trace explosives. Sampling that preserves the sample, has an understood efficiency for delivering samples to the detector, and meets constraints encountered in the field, has been dramatically improved though developments in measurement science.

In addition to these efforts, NIST has worked to develop a suite of Reference Materials and Protocols that can be used to assess the performance of instruments in the field. These materials and protocols are regularly used by TSA to assess the performance of their instrumentation, and are also being evaluated by the Bureau of Prisons and the State Department for possible use in assessing their instrumentation and training their operators.

NIST continues to make advances in this space and we are currently working to develop the tools that will enable a move to more non-intrusive sampling proceeds. As an example, NIST staff are currently working on solving the measurement challenges that must be overcome to incorporate trace explosive detection methods into credit card readers.

Chemical and Biological Threat Detection - Together with DHS, the Centers for Disease Control and Prevention (CDC), the National Institutes of Health (NIH), and EPA, NIST scientists are working on multiple projects to develop both improved sensor technologies and validated standards and procedures to assist local, state and federal agencies in the detection and response to chemical and biological threats. Examples of NIST work in this space include the following.

- NIST has been working with DOD and others to develop characterization tools to improve the sensitivity and reliability of the detection of numerous bioagents and toxins. Previous collaborations with NIST and the U.S. Army Dugway (Utah) Proving Ground have developed reliable methods based on DNA analysis to assess the concentration and viability of anthrax spores (Bacillus Anthracis). The techniques and data developed through this collaboration are essential steps in developing a reliable reference standard for anthrax detection and decontamination.

- In the wake of the Anthrax attacks, the first responder community needed better guidance and protocols to enable effective detection of biothreat agents during response and decontamination operations. Working with DHS, ASTM International, and the Association of Analytical Communities (AOAC International), NIST led the effort to develop the ASTM E2458 standard for the bulk sample and swab sample collection for suspected biological threat agents and ASTM E2770 for operational guidelines for the initial response to a suspected biothreat agent. NIST is an active contributor to a DHS-led workgroup comprising also CDC, EPA, and DOE national labs to improve the Federal guidance on validation and use of environmental B. anthracis collection methods.

- Work at NIST in the area of Microelectrical Mechanical Systems (MEMS) and microfluidics is being leveraged by DOD, DHS, and EPA in the development of systems to detect trace amounts of chemicals or toxins in air and water.

Radiological and Nuclear Threats -- With new technologies emerging for detection of radioactive materials, NIST has been active in development of new detection standards. NIST has partnered with both ANSI and the International Electrotechnical Commission (IEC) to facilitate the development of Documentary Standards for portal and handheld detectors for radioactive materials. In addition, NIST has developed calibration capabilities and reference materials, so the performance of the radiation detectors can be reliably ascertained, by DNDO. NIST is working with DNDO and DOD to develop a program for testing commercial off the shelf radiological and nuclear detection instruments in an effort to the implement the 2011 National Strategy for CBRNE Standards, which represents the Federal consensus regarding CBRNE countermeasures standards.

Closing Remarks

Standards play an important role in reliable threat detection, as they establish the reproducibility of the measurement, comparability of measurements made at different locations with different technologies, and the comparability of historical data to the data available today.

Standards are important in quantifying the level of confidence that can be placed in the data.

NIST's focus is on measurement. With deep expertise dealing with measurement repeatability and uncertainty in such wide-ranging areas as Chemical, Nuclear, Biologic, and Explosives, we are well positioned to support the measurement assurance needs of academia, industry and other federal agencies. We do this through the development of standards, guidance and reference materials, and by providing technical advice when and where needed.

In conclusion, NIST expertise in measurement science and standards is playing a recognized role in providing the country with robust threat detection capabilities.

Thank you, again, for the opportunity to testify today. I would be happy to answer any questions you may have.

Chairman HALL. I do thank you, and I thank you a good opening statement because that indicates to us, I think, the importance of your testimony here today, important not just to this Committee or to this Congress but to people everywhere. You know, we start our weeks off going through detection equipment. I go through Dallas, and it seems like they have different rules every doggone Monday. I was so pleased when they told me last Monday that if I was born before 1982, I could keep my shoes on, and you know, you have to be careful. I am sure those things are important, but this is what people are watching and looking for and complaining about, and I think this is probably one of the most important hearings that we are going to have to date as far as the rest of the people, all the people, a majority of the people are interested in.

So with that, I recognize Dr. Gowadia to present her testimony, and I hope I have been pronouncing your name right.

Dr. GOWADIA. You have, sir. Thank you.

Chairman HALL. You are recognized for five minutes.

STATEMENT OF DR. HUBAN GOWADIA, ACTING DIRECTOR, DOMESTIC NUCLEAR DETECTION OFFICE, DEPARTMENT OF HOMELAND SECURITY

Dr. GOWADIA. Good morning, Chairman Hall, Ranking Member Johnson and distinguished Members of the Committee. Thank you for this opportunity to discuss advances we have made in science supporting nuclear threat detection at the Department of Homeland Security's Domestic Nuclear Detection Office. At DNDO, with its singular focus on nuclear terrorism, we work with federal, state, local, tribal, international and private-sector partners to reduce the risk by making nuclear terrorism a prohibitively difficult undertaking for our adversaries.

Our ability to counter the nuclear threat is fundamentally based on the critical triad of intelligence, law enforcement and technology. DNDO contributes to this mission by analyzing and coordinating the global nuclear detection architecture and implementing its domestic component. We also conduct research, development, test and evaluation for threat detection technology, acquire and deploy it, and support and assess its operation once it is in the field. To maximize our ability to detect and interdict nuclear threats, it is imperative that we apply these technologies and operations that are driven by intelligence indicators and place them in the hands of well-trained law enforcement and public safety personnel.

Consequently, we are focusing on an architecture that is capable of surging in response to credible information that indicates an imminent threat to our national security. This means that nuclear detection capabilities must be robust, flexible, agile and well-coordinated. We have steadily increased our collaboration with the intelligence community. By sharing information, personnel and requirements we continue to improve our ability to successfully bring technologies to bear on the nuclear detection mission.

The success of our detection architecture is also dependent on the work and vigilance of law enforcement and public safety personnel who are appropriately trained and well-equipped for this mission. Not only is DNDO setting the training standards and building the curricula necessary to train frontline operators, we support the technological breakthroughs that give them the necessary nuclear search and detection tools.

For example, DNDO led the development of a next-generation radioisotope identification device. We worked closely with our partners to identify key operational requirements that drove the new system design. It is based on an enhanced detection material, lanthanum bromide, and coupled with improved algorithms. This new hand-held technology is easy to use, lightweight and more reliable, and because it has built-in calibration and diagnostics, it has a much lower annual maintenance cost.

One of our interagency leadership successes has been our response to the helium-3 shortage. Thanks to our research, development, test and evaluation efforts, DNDO has proven that alternative technologies for neutron detectors are both feasible and now available for integration into radiation portal monitors. Importantly, due to a collaborative government-wide effort, our U.S. strategic reserve of helium-3 has increased 40 percent since 2009.

Of course, an adversary can complicate the detection mission by shielding or masking the nuclear threat. To address shielded nuclear threats, DNDO has several projects underway. One, the Shielded Nuclear Alarm Resolution project, seeks to develop and characterize advanced active interrogation systems with improved ability to uniquely detect special nuclear material and to resolve alarms with confidence, even in the presence of significant countermeasures. As we implement a more agile architecture, we will need cost-effective detectors that can be widely deployed and detection systems that can search wide areas, even in the most challenging environments such as along our land, air and sea borders.

Such challenges require new materials that can be applied in novel concepts of operation. DNDO successes here include exploiting emerging detector crystals such as strontium iodide and cesium lithium yttrium chloride to improve our detection localization and identification of radiation sources.

DNDO's technology contributions to the global nuclear detection architecture start with cutting-edge research, predominantly executed through our transformational and applied research portfolio which lays the foundation for our development mission. This results in a program of progression that touches almost every one of DNDO's directorates. Paramount to this technical progression is our rigorous test and evaluation program that assesses equipment against established national and international standards.

DNDO is able to strengthen the security triad of intelligence, law enforcement and technology because of our integrated and holistic approach to the nuclear threat detection mission. Our disciplined and singular focus on nuclear counterterrorism is reinforced by a rigorous systems development process and anchored by the skills and knowledge of our interagency staff of scientists, engineers, current and former law enforcement and military personnel, intelligence professionals and policy experts.

Thank you again for this opportunity to discuss DNDO's efforts to protect our Nation from the nuclear threat. I will be happy to answer any questions from the committee.

[The prepared statement of Dr. Gowadia follows:]

Written Statement

of

Huban A. Gowadia, PhD
Acting Director
Domestic Nuclear Detection Office
Department of Homeland Security

Before the House Committee on Science, Space, and Technology

Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies

July 19th, 2012

Huban A. Gowadia
Before the House Committee on Science, Space, and Technology
July 19, 2012

Good morning Chairman Hall, Ranking Member Johnson, and distinguished Members of the Committee. As Acting Director of the Department of Homeland Security's (DHS) Domestic Nuclear Detection Office (DNDO), I am pleased to testify today with my distinguished colleagues to discuss ongoing research and development of nuclear detection technologies.

DNDO is a unique interagency organization with staff expertise in technical, law enforcement, military, and interagency issues focused exclusively on preventing nuclear terrorism. Countering nuclear terrorism is a whole-of-government challenge, and DNDO works with Federal, state, local, tribal, territorial, international, and private sector partners to fulfill this mission. Working with partners from across the U.S. government (USG), including the Departments of Energy (DOE), State (DOS), Defense (DOD), Justice, the Intelligence Community, and the Nuclear Regulatory Commission, DNDO coordinates the development of the global nuclear detection architecture (GNDA) and implements the domestic portion of the architecture. DNDO also works with its partners to coordinate interagency efforts to develop technical nuclear detection capabilities, measure detector system performance, ensure effective response to detection alarms, integrate USG nuclear forensics efforts, and conduct transformational research and development for advanced detection and forensics technologies. We coordinate and collaborate efforts through shared review of Broad Area Announcements, Requests for Proposals, and through interagency portfolio reviews. Additionally, we interact and exchange technical information for research and development efforts under a Memorandum of Understanding with relevant parties.

Detecting Nuclear Threats

Along with intelligence and law enforcement, technology is fundamental in our ability to detect nuclear threats. In recent years, there have been dramatic advancements in nuclear detection technology. Thirty years ago, identification of detected nuclear material required laboratory specialists and large, complicated equipment. Now, however, newer detection materials that can be integrated into mobile and human-portable devices, coupled with advanced algorithms, allow for significantly improved operations. As a result, frontline responders and law enforcement officials now regularly use detection equipment to search for, find, and identify nuclear materials in the field. Technological advances in computing, communications, software, and hardware have also contributed to this revolution in nuclear detection technology.

Despite these advancements, however, developing nuclear detection technology for homeland security applications is an inherently difficult technical task. The fundamental technical challenge for nuclear detection is one of distinguishing signal from noise. Sensors can detect radiation, but detection is limited by several factors, including speed, distance, shielding, and source strength. Compounding these challenges is the difficulty in distinguishing ever-present background radiation from radiation that poses a threat.. Additionally, to mitigate risk across all pathways in the GNDA, detection technologies must be capable of operations in challenging environments, such as on the water and in rugged terrain between ports of entry.

Current Nuclear Detection Systems

Currently, there are several types of passive detection systems deployed across the GNDA by federal, state, and local entities. For example:

- Personal Radiation Detectors (PRDs) are generally small, pocket-sized devices used as scanning tools to search for and detect nuclear and radiological materials.
- Hand-held Radioisotope Identification Devices (RIIDs) are designed to identify the radionuclides present in radioactive materials and sources and are used by law enforcement officers and technical experts during routine operations.
- Radiation Portal Monitors (RPMs) are large, usually fixed, detectors typically composed of polyvinyl toluene (PVT) for gamma detection andhelium-3 tubes for neutron detection, and are often used to scan vehicles or cargo at fixed chokepoints such as ports of entry and weigh stations.
- Mobile and Transportable Detectors, are mounted in a ship, vehicle, or trailer and used for area surveillance, search, or temporary checkpoint deployments.
- Backpack Based Radiation Detection systems - are used in mobile or checkpoint operations to search for nuclear threat materials.

To further improve operational nuclear detection capability, DNDO led the development of a next-generation RIID. We worked closely with U.S. Customs and Border Protection (CBP), the United States Coast Guard (USCG), the Transportation Security Administration (TSA), and state and local operators, to identify key operational requirements that drove the design of the new system. Based on an enhanced detection material, lanthanum bromide, and improved algorithms, this new handheld technology is easy-to-use, lightweight, and more reliable, and because it has built in calibration and diagnostics, has a much lower annual maintenance cost.

In addition to the aforementioned passive detectors, radiography imaging systems are used to help identify threats or anomalies in cargo and conveyances. These systems employ x-rays or gamma rays to image conveyances. The images generated by currently-deployed technologies must be reviewed by trained and skilled operators to ascertain anomalies that might indicate threat materials- a time-consuming process. DNDO is presently developing algorithms to automatically detect nuclear threats and shielding that may be used to conceal these materials.

Our ongoing collaboration with CBP to facilitate container security has resulted in the radiological and nuclear scanning of over 99 percent of all incoming containerized cargo transported via truck at land border crossings and at our seaports, utilizing RPMs. DNDO has procured thousands of PRDs, RIIDs, and backpack detectors for CBP, USCG, TSA, as well as for state, local, and tribal law enforcement across the country to scan people and their effects, cars, trucks, and other conveyances for the presence of radiological and nuclear materials. In addition, all TSA Visible Intermodal Prevention and Response teams and USCG boarding teams are now equipped with radiation detection capabilities. Additionally, to ensure the detection systems are used effectively, DNDO has made available radiological and nuclear detection training to over 23,000 state and local law enforcement officers and first responders.

Recognizing the important contributions and innovations of private industry, national laboratories, and academia, DNDO has evolved its acquisition focus from one that is predominantly fueled by a government-funded, government-managed development process to one that relies upon industry-led development. As such, all DNDO technology development programs now proceed with a "commercial first" approach – engaging first with the private sector for solutions and only moving to a government-sponsored and managed development effort if necessary. This approach takes advantage of industry's innate flexibility and ability to rapidly improve technologies, leveraging industry-led innovation.

This transition will also include a new approach at the systems level, in which strategic interfaces will be clearly defined in the detector/system architecture, allowing system upgrades without wholesale changes. We have shared the DNDO Acquisition and Commercial Engagement Strategy with industry through DHS's Private Sector Office to ensure the commercial sector remains aligned with DNDO's current development and acquisition approach. In some cases, shifting to commercial-based acquisitions will reduce the total time to test, acquire, and field technology.

Next Generation Nuclear Detection Systems

While DNDO's work to develop, evaluate, and deploy systems supports the ongoing enhancement of the GNDA, significant technical challenges remain. These challenges include:

- Cost effective equipment with sufficient technical performance to ensure widespread deployment;
- Enhanced wide area search capabilities in a variety of scenarios to include urban and highly cluttered environments;
- Monitoring along challenging GNDA pathways, to include scanning of general aviation and small maritime vessels, and searching for nuclear threats between ports of entry; and
- Detection of nuclear threats even when heavily shielded.

Additionally, our programs must be able to reach out to operators for user requirements and to balance both "technology push" and "technology pull" efforts, as appropriate. For the former, the technology developer is pushing a new concept out for examination by the operator. These systems may be otherwise unknown to operators, and are often state-of-the-art with enhanced or dramatically improved threat detection capabilities and may further allow for simplified operational use. Technology pull refers to equipment and programs where operators have identified new concepts of operation and/or features that they need in order to achieve their missions. The operators are constantly pulling the technologies in directions that guide our development of detection systems.
DNDO works to address these challenges through a robust, long term, multi-faceted transformational and applied research and development (R&D) program. I would like to highlight a few of the projects in our transformational R&D portfolio that are showing significant progress and promise.

Helium-3 Alternatives

Helium-3 has been widely used as a neutron detection component for radiation detection devices, such as RPMs. However, in recent years, our country has faced a helium-3 shortage. Years before the recent helium-3 shortage, DNDO and the DoD Defense Threat Reduction Agency (DTRA) were already exploring options for better, more cost-effective, alternatives for neutron detection. DNDO's transformational and applied research efforts included fourteen different technologies that could be used instead of helium-3 tubes, including those based on boron or lithium.

Once the shortage was identified, DNDO accelerated this progress and led an interagency working group to address the use of alternate neutron detection technologies. DNDO also queried the commercial marketplace for available systems. At a recently-completed test, present and next generation alternatives from the interagency research and development portfolio and the private sector were evaluated and multiple systems proved to have sufficient performance to replace helium-3 in RPMs. As a result of our efforts, alternative neutron detection technologies are now commercially available and large quantities of helium-3 will no longer be necessary for use in RPMs. Importantly, due to a collaborative, USG-wide effort to address the shortfall, our U.S. strategic reserve of helium-3 has increased by 40% since 2009.

Advanced Radiation Monitoring Device (ARMD)
Our Advanced Radiation Monitoring Device (ARMD) project focuses on enhancing our ability to distinguish benign radiological and nuclear materials, from those that potentially pose a threat. The ARMD project capitalizes on the efficiency and energy resolution of emerging detector crystals, such as strontium iodide (SrI_2) and cesium lithium yttrium chloride, or "CLYC", to develop smaller, more capable detection systems. The detector materials have sufficiently matured to the point where they are now commercially available – the direct result of a coordinated interagency effort between DNDO, DTRA, and DOE. New handheld detector systems using these crystals are being designed, built, and will soon be ready for formal evaluation by DNDO.

Long Range Radiation Detection (LRRD) Project
Our Long Range Radiation Detection (LRRD) project has the potential to have broad operational impact by significantly improving the range of detectors. Through the LRRD project, DNDO has been developing advanced technologies to detect, identify, and precisely locate radiation sources at stand-off distances, through passive gamma-ray imaging technology. We have focused on two systems: Stand-Off Radiation Detection Systems, which uses a mobile system to locate stationary sources; and the Road Side Tracker, which is a rapidly re-locatable monitoring system capable of identifying and tracking threats in moving vehicles across multiple lanes of traffic. Recent LRRD demonstrations included interagency partners from the technical and law enforcement communities, utilizing a "technology push" to allow operators to use the prototype systems in simulated and operational environments. DNDO is assessing the potential for further development based upon operator feedback and evaluations obtained during the demonstrations.

Networked Detectors
To address nuclear detection in challenging operational environments, DNDO is working on networked detectors. These detectors, being developed in the Intelligent Radiation Sensor System (IRSS) project, are intended to facilitate situational awareness and improve capabilities to detect, identify, locate, and track threats across distributed sensors. The IRSS integrates data from across multiple portable detectors with the goal of improving overall system performance

compared to a non-networked system. This technology will support operations where scanning for nuclear threats by routing traffic through checkpoints is not tenable. These operations include nuclear searches at some special security events, between ports of entry along the land border, or scanning general aviation or small maritime vessels for illicit radiological or nuclear materials.

Detecting Shielded Nuclear Threats

Nuclear threats may be shielded or masked, increasing the challenge for passive detection techniques. To address shielded nuclear threats, DNDO has several important projects. The Shielded Nuclear Alarm Resolution (SNAR) project seeks to develop and characterize advanced active interrogation systems with improved ability to uniquely detect special nuclear material and to resolve alarms with confidence, even in the presence of significant countermeasures (such as shielding). The scanner systems generate X-rays and/or neutrons, which pass through the cargo container and interact with the materials inside. These interactions can produce high-resolution images that reveal the shapes of objects inside the container. The scanner systems can also produce physical signatures, which uniquely identify materials inside, including those that can be used to make nuclear weapons or shield nuclear materials from detection.

This technology may substantially reduce the number of manual inspections required to resolve alarms, while increasing the probability of nuclear threat detection even when heavily shielded. Technologies under review include induced fission, high energy backscatter, and nuclear resonance fluorescence. Characterization activities for all SNAR systems will conclude in late 2012.

Recent advancements in the commercial sector have also resulted in technologies that combine the merits of passive and active technologies into a single system through either muon tomography or by integrating radiation detectors into x-ray radiography systems. In theory, these systems should be able to automatically detect nuclear threats, regardless of the shielding level, while providing an image for detecting other anomalies. In order to characterize the full performance capability of these technologies, DNDO recently solicited proposals for our Nuclear and Radiological Imaging Platform Advanced Technology Demonstration. This project will characterize imaging systems for scanning conveyances and identifying possible shielded threats. Results from this demonstration will be available in 2014.

Testing, Evaluation, and Standards for Nuclear Detection Technologies

Over the years, DNDO's test program has grown and matured. To date, DNDO has conducted more than 70 test and evaluation campaigns at over 20 experimental and operational venues. These test campaigns were planned and executed with interagency partners using rigorous, reproducible, peer-reviewed processes. The interagency involvement in these tests is underscored by DNDO's use of a DTRA test director for the DNDO Dolphin test campaign. Tested nuclear detection systems include pagers, handhelds, portals, backpacks, and vehicle-, boat- and spreader bar-mounted detectors, as well as next-generation radiography technologies. The results from DNDO's test campaigns have informed federal, state, local and tribal operational users on the technical and operational performance of nuclear detection systems, allowing them to select the most suitable equipment and implement effective concepts of operations to detect nuclear threats.

DNDO has also supported the development, publication and adoption of national consensus standards for radiation detection equipment. Several such standards now exist for use in homeland security. DNDO collaborated with the National Institute of Standards and Technology (NIST) to conduct a review of all national and international consensus standards for nuclear detection systems, and formed an interagency working group to draft government-unique technical capability standards (TCS). Earlier this year, we finalized the first TCS for handheld systems.

The success of the nuclear detection mission is contingent on timely information exchanges.. To this end, DNDO successfully collaborated with the NIST to create a major update of the Data Format Standard for Radiation Detectors used for Homeland Security. This standard facilitates the exchange of detection information by ensuring that the systems create and distribute data in a specified format to enable interoperability. Through the International Electrotechnical Commission (IEC) and the American National Standard Institute/Institute of Electrical and Electronics Engineers (ANSI/IEEE), this significantly improved standard (ANSI/IEEE N42.42 and IEC 62755) is now internationally accepted. IEC 62755 was approved in late February 2012.

The DNDO Graduated Radiological/Nuclear Detector Evaluation and Reporting (GRaDER^{SM}) Program builds upon these standards to determine if commercially-available nuclear detection equipment complies with established standards. DNDO created the infrastructure for voluntary, vendor testing of commercial nuclear detection technologies by independent, National Voluntary Laboratory Accredidation Program (NVLAP) accredited laboratories against national consensus standards and government-unique TCS. This program encourages vendors to develop better nuclear detection and identification systems that meet evolving Homeland Security requirements.

With the maturation of our test and evaluation program, DNDO's collaboration with interagency partners, such as DOE and DOD, and international partners, such as the United Kingdom, Canada, Israel, the European Union (EU), and the International Atomic Energy Agency (IAEA)), has increased significantly. For example, our close partnership with the DOE Second Line of Defense program, EU, and the IAEA for the Illicit Trafficking Radiation Assessment Program+10 (ITRAP+10) will result in a comprehensive evaluation of the performance of nearly one hundred commercially-available radiation detection systems against national and international standards. ITRAP+10 will allow for the refinement of nuclear detection standards and promote greater homogeneity in US and international detection standards. The test program will conclude in the spring of 2013.

Academic Research

In recent years, statistics have indicated a frailty in the expertise pipeline for fields important to national security—especially those that impact DNDO's mission spaces for nuclear detection and technical nuclear forensics. In recognition of this important need, DNDO seeks to support students and programs that address nuclear detection and forensics related work. Underlying DNDO's R&D efforts is our Academic Research Initiative (ARI), a program executed in partnership with the National Science Foundation that seeks to ensure a continued pipeline for national human capital development. Since its inception in 2007, 57 grants have been awarded to over 45 academic institutions across the country. In fiscal year (FY) 2011, the ARI program supported 39 grants and over 150 students. Currently, the ARI has awards with 25 universities through 32 grants supporting 80 students. DNDO has worked hard to maintain ARI, despite significant fiscal constraints in FY 2012. The FY 2013 President's Budget Request includes funding for sustainment of the ARI program, with the potential for additional grantees.

The ARI projects and research support the technological breakthroughs that allow us to better accomplish our mission. ARI grantees are addressing fundamental research for passive and active detection, as well as nuclear forensics activities. The priorities being addressed through ARI projects include: advanced materials research; neutron detector alternatives to helium-3; advanced algorithms for a range of applications; detector modeling; research to support non-destructive inspection and active interrogation; and investigating novel techniques for detection, localization, identification, and characterization of radiological and nuclear sources. Many of these projects provide the early applied research necessary to support future capabilities needed to implement the GNDA.

Conclusion

DNDO has come a long way since its creation in 2005. With our integrated approach to GNDA planning, testing and assessments, research and development, and operational support, we continue to strengthen the nation's capabilities to detect and interdict nuclear threats. We appreciate your continued support as we work with our partners to develop and deploy the necessary systems to implement a nuclear detection architecture that can effectively respond to credible intelligence and threat information. In addition, we appreciate your continued support as we continue to research and develop technologies that meet the operational requirements of our end users.

Thank you for this opportunity to discuss our research and development of nuclear threat detection technologies. I would be happy to answer any questions from the Committee.

Chairman HALL. And we thank you, Dr. Gowadia.

I now recognize Dr. Peurrung for five minutes to present his testimony.

STATEMENT OF DR. ANTHONY PEURRUNG, ASSOCIATE LABORATORY DIRECTOR, NATIONAL SECURITY DIRECTORATE, PACIFIC NORTHWEST NATIONAL LABORATORY

Dr. PEURRUNG. Chairman Hall, Ranking Member Johnson and distinguished Members of the Committee, thank you for the opportunity to contribute today. I have devoted much of my career to ensuring that science has impact on national security missions and therefore it is an honor and a pleasure to testify on the critical role of science in the development of threat detection technology.

DOE's science laboratories strive to accelerate the rate of innovation, steward unique national capabilities and leverage our science base for the benefit of missions such as energy and security. Success also requires that we bring together university and industrial partners as well as a deep understanding of operational missions. The threat detection research programs at Pacific Northwest National Laboratory nicely illustrate how these objectives can come together.

We have scientific strengths and historic capabilities with roots in the Manhattan Project. In this setting, the lab has grown such that roughly half of our activity is focused in support of national security. Threat detection research has been central in this and remains an area where science plays a critical role. I am particularly proud of our work to deliver transformational change in the longer run so that grand challenges are addressed and our country will be ahead of its adversaries.

I will illustrate these points now with three examples. The role of science in the area of ultra-sensitive nuclear detection has been particularly rich and distinguished. Over four decades our ability to detect trace nuclear materials has improved dramatically to the point that we can now measure radioactive materials 100 million times less concentrated than those naturally present in this room. This effort is supported not only by security mission stakeholders but also by DOE's Office of Science as part of their fundamental physics programs. Shortly after the tragedy of Fukushima, we were able to detect the leading edge of a radioactive plume over U.S. territory, providing timely and critical information to decision makers.

My second example is detection materials. A helium-3 shortage recently threatened to diminish our national ability to detect nuclear threats. In conjunction with industry and several federal agencies, the DOE labs played critical roles in driving innovation and evaluating technology so that today needs are met with commercial instrumentation that does not consume precious helium-3. For the longer run, we are focused on the science that will explain how and why radiation detection materials function as they do. This will accelerate the future discovery of useful new materials.

Airport security provides my final example. Millimeter wave scanning dates back to the 1960s when researchers pioneered the development of optical and acoustic holography. While this technology was transitioned to commercial production, we retain capability that still drives innovation today. In the future, we anticipate providing the ability to detect concealed objects under a much wider range of scenarios. DHS and DOD, for example, have jointly supported a collaboration that promises to enable standoff detection of person-borne threats in crowds. Our combination of chemical science and explosives detection capability are leading to other breakthroughs such as novel vapor detection methods and novel X-ray signatures. Our vision is for a future with airport security technology that performs better and has less operational impact.

I have attempted to suggest attributes that are common to successful threat detection research programs. These include integration of world-class scientific capability and applied research. There must be effective collaboration with industry and mission users to ensure long-term impact. There should be a range of federal sponsors who each leverage and build upon what has come before.

Largely because of the strength of our national science base and its effective application to threat detection, we continue to be global leaders in this area. Ten years ago, a National Academy of Sciences report stated: "strengthening the national effort in long-term research that can create new solutions should be a cornerstone of the strategy for countering terrorism." I believe this has occurred with considerable benefit to our national security.

There are challenges as well. Science programs are not always easily integrated with threat detection research because of cultural differences between science that is open and global and programs that are frequently sensitive. The DOE science labs are ideally suited to take on this challenge, and I assure the Committee that the leadership team at Pacific Northwest National Lab will do so.

I would also add that science center threat detection programs are fragile. They can be harmed not only by the inevitable fluctuations in funding support but also by rapid shifts in the leading threat of the day or by excessively short-term objectives. I recommend that strategic stewardship of our threat detection research capabilities and the science that underlies them remain a high federal priority. I am optimistic that the tremendous benefits of science-driven innovation will continue to make our Nation safer. We will continue to develop threat detection technologies that are more effective and operationally attractive. We will retain an ability to react rapidly to new changing or elevated threats.

I thank the Committee again for your time and attention.

[The prepared statement of Dr. Peurrung follows:]

U.S. DEPARTMENT OF ENERGY

Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies

Testimony of Dr. Anthony J. Peurrung
Associate Laboratory Director, National Security Directorate
Pacific Northwest National Laboratory

before the
Committee on Science, Space, and Technology
United States House of Representatives

July 19, 2012

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Introduction

Chairman Hall, Ranking Member Johnson, and members of the committee, thank you for the opportunity to contribute to today's hearing. The topic of this hearing is critical to securing America through the advancement of threat detection technologies. My name is Tony Peurrung, Associate Laboratory Director of the National Security Directorate at Pacific Northwest National Laboratory (PNNL) located in Richland, Washington, adjacent to the Hanford Site. It is an honor to provide testimony on the role of the national laboratories in the national scientific enterprise.

PNNL is one of ten U.S. Department of Energy (DOE) national laboratories managed by DOE's Office of Science (SC). Our research strengthens the nation's foundation for innovation, and we find solutions for not only DOE, but for the U.S. Department of Homeland Security (DHS), the National Nuclear Security Administration (NNSA), the Department of Defense (DoD), the Intelligence Community (IC), other government agencies, universities, and industry. Our multidisciplinary scientific teams are brought together to address the nation's most pressing issues in energy, environment, and national security through advances in basic and applied science.

Role of DOE Laboratories

Since the attacks of September 11, 2001, our nation has focused on maintaining the security of the homeland and prevention of further terror attacks. All across the country, industry, academia, and government have worked in tandem toward this goal.

The DOE complex of national laboratories, which have been a centerpiece of the nation's research and development capabilities for over sixty years, have played a prominent role in developing and deploying detection technologies to protect America against evolving threats.

Important objectives of DOE's multi-program science laboratories are to accelerate the rate of innovation, steward unique national capabilities, and leverage the national science base for the benefit of diverse applied missions. The threat detection research programs at PNNL successfully illustrate how these objectives come together. We have scientific strengths and historic capabilities with roots dating back to the Manhattan project of the 1940s at the Hanford Site. Today, approximately half of PNNL's \$1.1 billion business is centered on national security missions. Threat detection technology development is a central part of these programs and one in which science plays a particularly critical role.

DOE labs combine deep scientific insight and a keen understanding of operational missions with strategic partnerships—including universities and industry—to develop novel detection technology. The laboratories are working to prepare for tomorrow's challenges and deliver transformational technological change so that today's detection challenges are addressed and our country stays ahead of adversarial threats.

Ultra-Trace Detection and Analysis

Ultrasensitive nuclear detection is an area where the interplay between fundamental science and detection technology has been particularly rich and distinguished. Over four decades our ability to detect and characterize trace nuclear materials had improved to the point that radioactive materials eight orders of magnitude less concentrated than those naturally present in this room can be measured. This continuing effort is supported by various security mission stakeholders and by DOE's nuclear physics and high-energy physics programs. For example, after the tragedy at Fukushima, we were the first to detect trace amounts of radioactive material over U.S. territory, providing timely and critical information for U.S. Government decision-makers.

As the steward for various national scientific capabilities, PNNL researchers have been evolving the Multi-Sensor Airborne Radiation System (MARS) to support nonproliferation objectives of the NNSA. The system was recently deployed on a helicopter—a first for a system with this level of precision. (MARS was previously demonstrated on a truck that traveled from Richland, Washington to Charleston, South Carolina, and then on two boats.) The technology advances the state of the art in radiological detection at standoff distances. Using high-purity germanium crystals inside a vacuum cryostat, MARS detects and identifies radiological isotopes, with great precision, from a distance of tens of meters. MARS sends its detection data to a computer in real time, where operators quickly can see what substance is being detected and how radioactive it is. Knowing that, experts can tell what kind of nuclear material is in the vicinity, where it is coming from, and how dangerous it is.

Materials Development

PNNL's understanding of radiation and materials allows researchers to make significant breakthroughs in radiation detection materials discovery and development for DHS's Domestic Nuclear Detection Office (DNDO). Both the scarcity of helium-3 (He-3) and the need for improved radiation detection has focused research on discovering new materials. The recent He-3 shortage threatened to diminish our national ability to detect nuclear threats. Several DOE labs, in conjunction with industry, the DNDO, and NNSA, played critical roles in driving innovation and evaluating technology so that today's detection system needs are met with commercial instrumentation that does not consume precious He-3. In the longer run, improved detection systems will require more rapid discovery of new materials with advanced capabilities. To this end, laboratories such as ours have focused on the fundamental science necessary to understand how and why radiation detection materials function as they do.

For example, over the last few years, PNNL has been using its expertise in materials discovery to identify, select, and develop new materials that will improve the resolution and processing time in detecting radiological and nuclear devices. Experts now have a greater understanding of the potential materials covering the four conventional semiconductor material classes. They were able to narrow over 2,000 material compositions to a list of 245 that may have comparable performance characteristics to cadmium zinc telluride, a well-known radiation detection material. This work has drawn collaborative interests from multiple industrial and academic partners with plans to develop new detection instruments, increasing effectiveness in the field.

Cyber Security

In the mid-1990s, a new DOE user facility—the Environmental Molecular Sciences Laboratory, or EMSL—came on line at PNNL and made state-of-the art research equipment available to researchers across the nation and around the world. The vision was to provide virtual access to this equipment so researchers would not have to be physically located at PNNL. This drove some of our initial work in cyber security. Today, major cyber attacks occur on a regular basis across the U.S. Cyber security researchers combat over 500 million events per day at 90 DOE sites. Their efforts are changing the paradigm away from reactive efforts to more proactive approaches through programs such as Digital Ants™. As the name suggests, this program provides a framework for decentralized coordination modeled on the real ant behavior known as "swarm intelligence." Cited as one of ten innovative technologies in "World Changing Ideas" in the December 2010 issue of Scientific American, the Digital Ants™ solution reduces the level of required human involvement in problem detection and resolution while retaining the human ability to intervene as desired. If the "ants", small computer programs, find a symptom, they wander through computers searching out and then swarming on viruses and worms. This novel, flexible approach reduces cyber threats for individuals, industry, and critical national infrastructures. In the longer run, PNNL researchers are striving to make a range of national infrastructure dramatically more resilient in a way that does not require inordinate cost or hinder normal operation.

Partnerships

The DOE laboratories actively engage academia and industry to advance threat detection technologies. A couple of examples include the DHS Science and Technology (S&T) Directorate and PNNL-led National Visualization and Analytics Center (NVAC) and DHS's Centers of Excellence. NVAC develops the advanced visual analytics capabilities to help respond to accidental, intentional, and natural disasters. NVAC coordinates with other such centers globally to bring a wide range of new technologies to bear through academic, government, industrial, and international partnerships. For example, NVAC supported DHS in the development of a formal U.K. Visual Analytics Consortium. Researchers from PNNL participated in the third International Workshop on Visual Analytics in September 2011 and the kickoff meeting of Visual Analytics for Security Applications. Both events provided an opportunity for the U.S. and Germany to discuss technical objectives and scope. NVAC also conducts collaborative research in visual analytics with the DHS S&T Command, Control, and Interoperability Center of Excellence co-led by Purdue University and Rutgers University.

DHS's Centers of Excellence draw upon expertise from the national laboratories, universities, and industry to advance technology, including advanced-imaging technologies (AIT, formerly known as whole-body imaging). The averted terrorist events of December 2009 hastened the deployment of these technologies which hold promise for detection of explosives at checkpoints (portals). Significant ongoing scientific challenges regarding personal privacy and automated threat detection are preventing widespread acceptance and deployment of these systems. Expertise in AIT exists within the national laboratory system, particularly at PNNL, as well as within the DHS Center of Excellence in Explosives, ALERT (Awareness and Localization of Explosives-Related Threats) located at Northeastern University. Leveraging these capabilities, PNNL is working with researchers, scholars, and university students as well as industry representatives to collaborate on AIT challenges.

Advances in Threat Detection

Significant advances in threat detection technology are ongoing, and there is an exciting vision for the future. New discoveries have the ability to transform the way threats are detected in such places as our airports and border crossings. It is also worth noting that detection research and development not only involves physical detectors, but also important areas such as the discovery of novel signatures and performing large-scale data analysis.

Improving Airport Security

One particular example of technology advancement is in airport security. PNNL's Millimeter Wave technology is helping to detect concealed weapons, explosives, and contraband. The roots of the technology date back to the 1960s when researchers at PNNL pioneered the development of optical and acoustic holography—the foundation of the millimeter-wave technology. In 1989, PNNL worked with the Federal Aviation Administration (FAA) to perform feasibility studies and the first patent was issued in 1995. Today, airport scanners are equipped with this detection technology across the globe.

In the future, the Millimeter Wave technology can be used in standoff detection of explosives and nondestructive detection and evaluation of objects under a much wider range of scenarios. For example, DHS and DoD jointly supported integrated research that promises to enable standoff detection of person-borne explosive threats in crowds. This effort involves partnership with the National Institute of Standards and Technology (NIST), the United Kingdom Home Office, and industry. Other breakthroughs such as novel vapor detection approaches and novel x-ray signature development continue to result from our combination of fundamental chemical science and applied explosive detection capability. PNNL continues to work with federal agencies and industry to expand the next generation of threat detection technology for aviation security.

Advancing Data Analytics

Another example is the nation's ability to analyze large volumes of heterogeneous data for potential threats. The analysis of data has evolved from yesterday's scenario of individuals reading volumes of printed materials to the use of electronic tools that visually represent data from disparate sources. Researchers are using visual and data analytics to study and understand the capabilities, motivation, and intent of our nation's adversaries. Our process uses data representations and algorithmic techniques from other basic and fundamental science domains and creatively applies them to national security problems. Flagship products like IN-SPIRE and Starlight, are now deployed to hundreds of U.S. Government analysts and used every day. Through these creative and powerful tools and methods, researchers are discovering new ways to detect relationships, trends and themes across many domains including cyber analytics, the electric grid, law enforcement, and systems biology. Tomorrow's tools will analyze not only text input from documents, websites, and social media tools but will address image, audio, video, and sensor data as well.

Complementary Work

The cross-cutting work that national laboratories conduct for one federal agency are often leveraged for the benefit of others. Examples include advancements in standoff detection technologies initially funded by DHS and now leveraged and funded by DoD, health research funded by the National Institutes of Health (NIH) that is now used in bioforensics research funded by DHS, and DOE seed investments—Laboratory Directed Research and Development (LDRD)—that focuses on discoveries for tackling the nation's greatest challenges.

Deployed Standoff Detection

One illustrative example of cross-cutting work is the Standoff Technology Integration and Demonstration Program (STIDP) at PNNL. This project was initially funded by DHS S&T in 2007 to develop and test an integrated countermeasure architecture to defeat person-borne improvised explosive devices (PBIEDs) using standoff technologies in an operational environment. Then in 2010, after a visit by DoD to the operational test site, there was a realization that the work being performed by PNNL for DHS was well beyond anything they were undertaking to detect improvised explosives in the battlefield. DoD is now funding this project exclusively and applying advances in standoff detection to the real-world. Partnerships include work with NIST, the United Kingdom Home Office, and industry.

Leveraging Medical Research

Medical research initially funded by NIH has been leveraged by DHS and others to advance bioforensics research. Viral pathogens are one category of a potential bioattack. PNNL is improving the detection of virus production signatures in bioforensic samples, via detection of proteins found in viruses. This project is using proteomics datasets and advanced mass spectrometric methods to analyze the *Vaccinia* virus. As stated by the Federal Bureau of Investigation's (FBI) Chemical Biological Sciences Unit, this work improves the detection of virus production signatures in bioforensic samples and fills an important gap in forensic method development.

Investing in the Future

The national laboratories invest in initiatives to deliver transformational science, technology, and impact; accelerate the rate of innovation; develop new partnerships for national and international impact; transform our science and technology workforce; and nurture and evolve the nation's core scientific capabilities. PNNL's LDRD program is a mechanism for bringing forward novel ideas that will become the next generation of science and technology. LDRD strengthens the nation's fundamental research component, builds capability in support of applied research and development programs, and translates scientific discoveries into real-world technology applications. One such investment is the Ultra-Sensitive Nuclear Measurement Initiative, which is focused on addressing the need for increasingly sensitive nuclear measurement systems to discover, analyze, and interpret extremely weak signals, including those from rare physical events. Another example is the Signature Discovery Initiative, which will deliver a systematic process and set of analytic tools to accelerate the discovery of new signatures in any domain, including threat detection. This research will produce an integrated analytic framework with new algorithms and methods for efficiently analyzing multisource data to uncover patterns and relationships that can be correlated with some measureable phenomena or event.

Conclusion

Shortly after the attacks of September 11, 2001, the National Academy of Sciences undertook a comprehensive study examining the importance of science and technology to tackle the multitude of threats to the homeland. The 2002 report entitled, *Making the Nation Safer*, stated "strengthening the national effort in long-term research that can create new solutions should be a cornerstone of the strategy for countering terrorism." I believe this has occurred with considerable benefit to our national security. Largely because of the strength of our national science base and its effective application to threat detection, we continue to be global leaders in this area.

There are challenges as well. Science programs are not always easily integrated with threat detection research because of cultural differences between the open, global scientific endeavor and programs that are frequently sensitive. The DOE national laboratories are ideally suited to take on this challenge and I assure the committee that the leadership team at PNNL will continue to do so.

Although extremely valuable, science programs targeted at pressing national security threats are fragile. They can be harmed not only by the inevitable fluctuations in funding support, but also by rapid shifts in the leading threat of the day or by excessively short-term objectives. I recommend that strategic stewardship of our threat detection research capabilities and the science that underlies them remain a high federal priority.

I am optimistic that the tremendous benefits of science-driven innovation will continue to make our nation safer. We will continue to develop threat detection technologies that are more effective and operationally attractive. We will retain an ability to react rapidly to new, changing, or elevated threats. I thank the committee again for their time and attention.

About the Speaker

Dr. Anthony (Tony) Peurrung is the Associate Laboratory Director of the National Security Directorate at Pacific Northwest National Laboratory (PNNL). Dr. Peurrung oversees the portfolio of national security programs and commercial enterprises at PNNL. Under his leadership, PNNL delivers scientific insights, tools and methods to deploy impactful science and technology to clients in the Department of Energy, Department of Homeland Security, Department of Defense, the Intelligence Community and the National Nuclear Security Administration.

Dr. Peurrung has contributed to a variety of fields within fundamental and applied physics including fluid mechanics, plasma physics, medical physics, separations science, environmental remediation, nuclear physics, and radiation detection methods and applications. His current research interests are centered on detection and characterization of special nuclear material, particularly problems where strong links to fundamental science capability are important.

About PNNL

Located in Richland, Washington, PNNL is one among ten U.S. Department of Energy (DOE) national laboratories managed by DOE's Office of Science. Our research strengthens the U.S. foundation for innovation, and we help find solutions for not only DOE, but for the U.S. Department of Homeland Security, the National Nuclear Security Administration, other government agencies, universities and industry. Unlike others, our multidisciplinary scientific teams are brought together to address their problems. More specifically, at PNNL we

- provide the facilities, unique scientific equipment, and world-renowned scientists and engineers to strengthen U.S. scientific foundations through fundamental research and innovation
- prevent and counter acts of terrorism through applied research in information analysis, cyber security, and the non-proliferation of weapons of mass destruction
- increase U.S. energy capacity and reduce dependence on imported oil through research of hydrogen and biomass-based fuels
- reduce the effects of energy generation and use on the environment.

Today, approximately 4,700 are employed at PNNL; our business volume is more than $1.1 billion. Our Richland campus includes unique laboratories and specialized equipment as well as the William R. Wiley Environmental Molecular Sciences Laboratory, a DOE Office of Science national scientific user facility. In addition to the Richland campus, we operate a marine research facility in Sequim, Washington; and satellite offices in Seattle and Tacoma, Washington; Portland, Oregon; and Washington, D.C.

Battelle—the world's largest independent scientific research and technology development organization—has operated PNNL for DOE and its predecessors since 1965. One unique feature of Battelle's contract with DOE allows research to be conducted for private industry.

www.pnl.gov

Chairman HALL. And I thank you.

And at this time I recognize our final witness for today, Dr. Peterson.

STATEMENT OF DR. THOMAS PETERSON, ASSISTANT DIRECTOR, DIRECTORATE FOR ENGINEERING, NATIONAL SCIENCE FOUNDATION

Dr. PETERSON. Thank you, Chairman Hall, Ranking Member Johnson and other distinguished Members of the Committee. It is an honor to be able to testify before you today on this topic of threat reduction and detection technologies.

I would like to briefly describe our efforts in this research area, both in terms of the investments made exclusively by NSF and in terms of important interagency partnerships we have, particularly with the Department of Homeland Security.

The primary mission of the Foundation is to support basic research in science and engineering as well as advancements in education in STEM disciplines. The NSF has the ability to reach deeply into the academic community across a broad range of areas to truly understand threat detection technologies requires expertise not only in engineering and physical sciences but in the life sciences, the social and behavioral sciences, and education as well, and NSF serves all these communities and our support in these areas taps into these particular strengths.

First, let me talk about our investments within the Foundation. A minimum of four directorates are heavily involved in advancing our understanding of threat detection and they are funded through engineering, computer information science and engineering, math and physical sciences, and social, behavioral and economic sciences. For example, the resilient and sustainable infrastructures cluster within engineering focuses on issues of importance in responding to both natural and manmade disasters. We support work on sensors and sensor networks, the fundamentals of sensor devices and technologies, the use of bioelectronics, optical imaging and optical devices based on metamaterials, and we support the development of mathematical and statistical algorithms and methodologies that are critical for these sophisticated sensor systems.

While much of the work continues to be supported through the core programs within the NSF, there have been specialized solicitations focusing exclusively on issues related to threat detection, and those solicitations have been in partnership with the Department of Defense and Department of Homeland Security. In collaboration with the DOD, work supported primarily by the math and physical sciences and social, behavioral and economic sciences directorates have examined the social and behavioral foundations of terrorism and the complex mathematical and statistical aspects of threat scenario analysis.

Perhaps our most significant contributions to this effort have come about through a longstanding and productive partnership with DHS. It is a program jointly executed by the Domestic Nuclear Detection Office and NSF and it was established via a memorandum of understanding in 2007. The Academic Research Initiative, as it is called, seeks to advance the fundamental knowledge for nuclear detection and related sciences. It is about a $60 million effort that has been groundbreaking collaboration between NSF and DHS on the detection of domestic nuclear threats. Example awards support the fundamentals behind methods to detect nuclear materials in large cargo containers and low-cost, effective, portable particle detectors that are systems to detect highly enriched uranium and other specialized nuclear materials.

Not all research focuses on detector technology. Some supported research utilizes a systems approach to design and analyze systems for detecting nuclear material at our Nation's ports. Collaborators at Texas A&M University conduct research involving the integration of social science and policy factors into detection systems, and efforts at UT Austin developed a new class of stochastic interdiction models on transportation networks. A second solicitation involving a DHS partnership, in this case, the explosives division of the Science and Technology Directorate, focused more specifically on explosives and related threats.

In conclusion, NSF continues to support fundamental research and education in science and engineering, particularly for areas and ideas generated by the academic community. Our ability to bring together a broad range of disciplines within that academic community is particularly beneficial in addressing complex issues such as the ones we are discussing today. By marshaling our expertise and collaboration with the strong mission-oriented foci of other agencies such as DHS, we have been able to contribute significantly, I believe, to advancing fundamental research relating to the detection of physical threats to our Nation and its people. In challenging budget times, partnerships such as this can often be threatened. It is my hope that we can continue to work collaboratively with our colleagues in DHS, DNDO and DOD and other agencies and to make valuable contributions to knowledge in this obviously important area.

I thank the Chairman and the Committee once again for the opportunity to highlight NSF's contributions and I would be happy to answer any questions.

[The prepared statement of Dr. Peterson follows:]

Testimony of

Dr. Thomas Peterson, Assistant Director
Engineering Directorate
National Science Foundation

Before the

U.S. House of Representatives
Committee on Science, Space, and Technology

Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies.

July 19, 2012

Chairman Hall, Ranking Member Johnson and other distinguished members of the Committee on Science, Space, and Technology, it is a pleasure to be able to testify before you today on the important topic of "Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies". I am Tom Peterson, Assistant Director for Engineering at the National Science Foundation. I would like to briefly describe our efforts in this research area, both in terms of investments made exclusively by NSF and in terms of important interagency partnerships we have, particularly with the Department of Homeland Security (DHS).

The primary mission of the Foundation is to support basic research in science and engineering, as well as advancements in education in science, technology, engineering and math (STEM) disciplinary areas. This mission to support *basic* research, independent of specific topical area, allows NSF to support creative and innovative ideas generated by the community in an incredibly broad spectrum of topics. At the same time, the Foundation has an obligation, as stated clearly in the NSF Act of 1950, "To promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes." So it is appropriate that some portion of our basic research investments touch on issues related to national security.

While the Foundation is comprised of seven directorates and four offices focusing on specific disciplinary research and education activities, the strength of the NSF is in our ability to reach deeply into the academic community across a broad range of areas. This "OneNSF" philosophy gives us the capability to advance science and engineering in ways that could not be done with a more focused, disciplinary or mission-oriented approach. To truly understand threat detection technologies requires expertise not only in engineering and physical sciences, but in life sciences, social and behavioral sciences and education as well. NSF serves all those communities, and our support in this area taps on all those strengths.

Support through Core Programs

First, important fundamental issues of advancing our understanding of threat detection are funded through the core programs in many divisions throughout the Foundation, particularly in Engineering (ENG), in Computer and Information Science and Engineering (CISE), and in Social, Behavioral, and Economic Sciences (SBE). For example, the "Resilient and Sustainable Infrastructures" cluster within ENG focuses on issues of importance in responding to both natural and man-made disasters. Understanding, for example, how social media and the ubiquitous presence of cell phones can help to mitigate the delayed response to disasters creating social disruption can help us improve our emergency management capabilities.

Another example of work funded in this area studies the technology for automatic detection and real-time mitigation of deliberate hazardous releases in infrastructure systems. This work can be used to help protect, in a reliable, cost-effective and socially acceptable way, passenger terminals, transportation tunnels, tall buildings or even a channel carrying water to a municipality. This work is being done at the University of Michigan.

Work on development of sensors and sensor networks is supported in a number of divisions and directorates, where the fundamentals of sensor devices and technologies are examined, as are the uses of bio-electronics, optical imaging and sensing, optical devices and components, and even optical devices based on meta-materials.

Work supported at the University of Utah focuses on unique configurations for gas chromatography to enable portable and high-capacity analyses of various airborne pollutants and contaminants, such as volatile organic compounds, thereby providing early warning for individuals.

And within our collaborative Industry University Cooperative Research Center (IUCRC) program, a biometrics center focusing on identification technology is supported at Clarkson University, West Virginia University, the University of Arizona and SUNY Buffalo. The center focuses on automated human biometric recognition in order to identify the actors likely associated with planning and executing asymmetric threats. The Center works closely with the Department of Homeland Security, the Department of Defense (DoD), the FBI and many other agencies.

While much work has been supported, and continues to be supported, through the core programs within the NSF, there have been specialized solicitations focusing exclusively on issues related to threat detection. Some of those solicitations are in partnership with DoD and DHS.

In collaboration with the DoD, work supported primarily by SBE at NSF has examined the social and behavioral foundations of terrorism, and includes for example, an award to the University of Maryland for the systematic analysis of unclassified empirical data on terrorist organizations, along with data on similar political organizations that choose not to use terrorism. Also supported was an award to the University of Texas-Dallas on the substantive expertise, strategic analysis and behavioral foundations of terrorism.

Partnerships with DHS

Perhaps our most significant contributions to this effort have come about through a long-standing and productive partnership with DHS. It is a program jointly executed by the Domestic Nuclear Detection Office (DNDO) and NSF, and it was established via a Memorandum of Understanding in 2007. Since the inception of this productive partnership, two distinct solicitations have been run.

The "Academic Research Initiative" seeks to advance fundamental knowledge for nuclear detection and related sciences, to develop human capital and address the graying of the nuclear science profession by training the next generation of nuclear engineers and physicists, and by sustaining a long-term commitment to frontier academic research in the field. This is about a $50 million effort that has been a groundbreaking collaboration between NSF and DHS on detection of domestic nuclear threats (aka, domestic nuclear terrorism). This solicitation has been run five times.

The second solicitation involving a DHS partnership (in this case, the Explosives Division of the Science and Technology Directorate) is "Explosives and Related Threats: Frontiers in Prediction and Detection".

Academic Research Initiative

The Academic Research Initiative partnership between NSF and DNDO of DHS has run a solicitation five times since its inception in 2007. The preponderance of investments have focused on the development of better and more sophisticated detectors for nuclear and actinide materials. Major technical challenges addressed by the efforts below include: radiation monitoring along the Nation's unattended land and sea borders; agile, mobile and re-locatable radiation detection and monitoring; unattended or ubiquitous radiation detection sensing systems; and high capacity, low dose scanning/screening technologies for cargo. For example:

- Researchers at Washington State University have investigated the effect of adding metallic nanoparticles to high-density scintillator materials to enhance the sensitivity and applicability of scintillator materials for nuclear threat detection.
- A research team from the City College of New York, Optical Semiconductors, Inc. and the Department of Energy's (DOE) Brookhaven National Laboratory combined efforts in spectroscopic characterization, material growth, and device manufacturing/testing to improve cadmium-magnesium-tellurium (CdMgTe) as the material of choice for room temperature gamma-ray detectors.
- A research team at UNC Chapel Hill and NC A&T is examining various techniques being developed to detect nuclear materials in large cargo containers based on gamma-ray beams to identify specific isotopes. High intensity gamma-ray beams with good energy resolution are expected to generate acceptable radiation doses to cargo and to enable scans to be performed in short enough times that make these techniques viable solutions. An ultimate goal is to apply this technology as the basis for systems that make isotope-specific images of high-Z materials in cargo containers.
- Purdue University researchers are trying to develop graphene-based sensors for detecting special nuclear materials because graphene is an electronic material with unique properties. Graphene-based radiation sensors have the potential to significantly outperform existing sensors for detecting special nuclear materials. Other researchers at Purdue are studying tensioned fluid metastable states as a basis for novel, transformational impact, low-cost, effective, portable particle detector systems to detect highly-enriched uranium and other

special nuclear materials. These "tensioned" metastable states in materials potentially offer unique, unsurpassed capabilities for detection.

- University of Hawaii researchers are evaluating the use of differential absorption and differential fluorescence for the detection of fissionable nuclear materials concealed by terrorists in shipping containers, road vehicles, aircraft and ships. Differential absorption and fluorescence have long been used effectively at optical and x-ray wavelengths to identify materials and structures that would otherwise be undetectable due to the higher levels of absorption or fluorescence by the materials in which the structures of interest are embedded.

Not all research focuses exclusively on detector technology.

- Researchers at Virginia Commonwealth University explored how a systems approach can be used to design and analyze systems for detecting nuclear material at our nation's ports. This research uses discrete optimization and decision analysis models to design multi-layered, risk-based, port security systems for detecting nuclear weapons and materials. Rutgers University addresses the issues of interpretation of data, responsive action, and managing the information generated by complex sensing systems. They address decision and control based on sensor information, and on incorporating uncertainty and risk into decision-making for use with imperfectly sensed data.
- Collaborators at Texas A&M University conduct research to demonstrate the ability to develop and deploy new detector concepts with fully integrated signal and information analysis to attain breakthrough improvements in the nation's ability to detect domestic nuclear threats. Their work involves (1) integration of social science/policy factors into the detection system parameter space, (2) enhancement of the education of undergraduate and graduate science and engineering students in areas related to nuclear security and border monitoring research, and (3) generation of self-sustaining research teams which will continue to expand fundamental knowledge in key nuclear detection fields.
- Efforts at UT-Austin are underway to develop a class of stochastic interdiction models on a transportation network consisting of two adversaries: a smuggler and an interdictor. The models are hierarchical, stochastic, and involve strategic gaming, and allow for testing of detection techniques employed by the interdictor and responses by the smuggler. The interdictor's goal is to minimize the probability the smuggler avoids detection. The intellectual merit of the work addresses stochastic interdiction optimization, probability and statistical modeling of uncertainties, and nuclear radiation transport modeling and analysis.
- Iowa State researchers are developing an informatics-based approach to the accelerated design and discovery of new radiation detector materials. The research integrates the formal methods of statistical learning in information theory to first-principles and mesoscale modeling, measurements of radiation detection characteristics, and novel high-throughput screening and modeling studies of defects in inorganic scintillator materials. This interdisciplinary collaborative is facilitated by a cyberinfrastructure for data sharing between Iowa State University (ISU), Case Western Reserve University (CWRU) and DOE's Los Alamos National Laboratory (LANL).
- Researchers at The University of Tennessee are addressing fundamental aspects of manufacturing technology that directly impact the affordability of the high-performance detection materials that are needed for effective high-speed scanning of cargo. Innovative synthesis techniques are being developed with the goal of improving the sensitivity and lowering the cost of materials that have the capability of uniquely identifying specific nuclear threats.

- A unique approach to nuclear forensics discovery is being taken at UC-Berkeley, where they are recasting nuclear forensics discovery as a digital library search problem. Nuclear forensics is the science of identification of source and characteristics of smuggled nuclear materials possibly seized by authorities. Nuclear material identification is of utmost importance to international threat reduction. The nuclear materials identification process will be cast as a search problem against a digital library of standard nuclear materials samples and their digital signatures.

Explosives and Related Threats: Frontiers in Prediction and Detection

A solicitation entitled "Explosives and Related Threats: Frontiers in Prediction and Detection" was issued by all seven directorates and two of the four offices within the Foundation. This solicitation followed NSF's investment in leading-edge frontier research on sensors and other areas, including the social and behavioral sciences that are potentially relevant to the prediction and detection of explosives and related threats. It sought to advance fundamental knowledge in new technologies for sensors and sensor networks, and in the use of sensor data and control systems in decision-making, particularly in relation to the prediction and detection of explosives and related threats. Examples of awards from that solicitation include:

- At Caltech, research to develop sensor arrays for vapor detection using chemically sensitive resistors and luminescent polymers together with biologically inspired algorithms to analyze and interpret the data. The work can potentially lead to a general purpose, trainable sensor.
- At the University of Connecticut, an ultra-thin molecular sieving zeolite membrane serves as an explosives vapor concentrator and single-walled carbon nanotube (SWNT)-porphyrin conjugates serve as sensing elements. These and other features promise to impart onto the electronic nose an unprecedented speed, sensitivity and selectivity, as well as a technology that can be readily miniaturized and applicable for remote surveillance devices.
- Researchers at GaTech are developing integrated planar optical waveguide spectrometry-interferometry for sensing explosives with imprinted polymers. Synthesis of molecularly imprintable polymers with reactive groups increase signal to noise and selectivity of the compounds to be detected.
- Collaborators at Princeton and George Mason University are working on improving nuclear quadrupole resonance (NQR) detection of explosives. NQR is desirable as it is a penetrating method of detection, and a practical implementation is addressed with the conceptual design of a device which mounts under a floor.

Conclusion

NSF continues to support fundamental research and education in science and engineering, primarily for ideas generated by the academic community. Our ability to bring together a broad range of disciplines within that academic community is particularly beneficial in addressing complex issues such as the ones we are discussing today. By marshalling our expertise in collaboration with the strong mission-oriented foci of other agencies such as the Department of Homeland Security, we have been able to contribute significantly, I believe, to advancing fundamental research relating to the detection of physical threats to our nation and its people. In challenging budget times, partnerships such as this one can be threatened. It is my hope that we can continue to work collaboratively with our colleagues in DHS/DNDO, DoD, and other agencies, and to make valuable contributions to knowledge in this obviously important area. I thank the Chairman and the committee once again for this opportunity to highlight NSF's contributions. I would be happy to answer any questions.

Chairman HALL. All right, and we thank you, and I thank all of you for your testimony. I remind Members that Committee rules limit our questioning to five minutes. I certainly will stay with the five minutes. At this time I will open the round of questions, and I recognize myself for five minutes.

Secretary Napolitano has asked for a delay in compliance with a 2007 requirement that all marine port cargo containers be scanned prior to U.S. entry. I think you all are familiar with that. And day to day we have complaints all across this country as to how they search them, and some question searching a 2-year-old, but we have knowledge and you all have the knowledge that people have used their children sometimes without any care or love of their own children to do harm to the enemy, and the enemy is us.

And I understand that currently less than one percent of the cargo is screened, and that is a frightening thing. I am aware of the commercially developed technology that exists that have the potential to help the government meet this requirement, but my question is, is there a way to expedite this process to find a solution more quickly? And do you anticipate that this problem is going to be solved by technologies developed by the government or by the private sector? I will let any one of you—start off with you, Dr. Cavanagh, if you would like to answer that. Go ahead and turn your microphone on.

Dr. CAVANAGH. I will get this straightened out, the high technology.

I don't believe NIST has a contribution to make to this question. I think my colleagues are better prepared to answer that.

Chairman HALL. Okay. We gave you a chance.

Dr. GOWADIA. Chairman Hall, probably the best part of DHS to answer to this question is probably our partners our Customs and Border Protection and our policy directorate. I do know that we did a pilot, the notion of 100 percent scanning overseas and there were some significant challenges that were predominantly diplomatic challenges and some pushback from international trade and possibly the need for border reconfigurations should reciprocity be required of us. I do believe that there are some technologies available for scanning but scanning of cargo rapidly and efficiently continues to be a bit of a challenge for us. So I think that is about as far as I can go, and I think it would be a question best answered by the Department itself.

Chairman HALL. Okay. And I thank you for that.

Dr. PEURRUNG. So I have personally been to foreign ports and observed their operations largely in connection with our laboratory's work for the NNSA's programs that involve global security reduction, second line of defense, those kinds of programs. It is clearly a significant challenge, what you pointed out. I would only say that the laboratories are working on advanced technology that should have an impact in the long run. This is one of these hard problems that calls for transformational technology. I can't promise anything in the extremely short-term future but there is promise in the long term.

Chairman HALL. All right, sir. Do you have anything to add to it?

Dr. PETERSON. No, I don't think NSF would have a specific contribution in this area.

Chairman HALL. Okay. I still have time to ask another question.

I hate to keep going back to the airports, but that is the connection I have with the searches and the complaints are based on things that happen at different airports, and the public is probably most aware of threat detection technology at the airport because people are flying right, left and sideways, and I guess to what extent is threat detection today going on behind the scenes and how is threat detection research and development balanced between detecting materials carried by individuals and detecting materials in cargo? Is there anyone here that feels that they can give me an answer to that?

Dr. GOWADIA. I will take a small shot at it.

Chairman HALL. I am glad they brought you.

Dr. GOWADIA. Thank you, sir.

Chairman HALL. I am going to tell you a story about searches too in just a moment when we have a little more time. Go ahead.

Dr. GOWADIA. I look forward to that.

At DNDO, we have worked very closely with our partners at the Transportation Security Administration. Every one of their VIPR teams, their visible—I should have this acronym down but I don't. But their VIPER teams are equipped with rad-nuke detection equipment and they are available to enter not just into the airport system but also into the other transportation modes domestically. So from a rad-nuke perspective, yes, we do work with TSA on that count, and we of course do work with our Customs and Border Protection colleagues to deploy detectors in air cargo.

Chairman HALL. And I thank you. I yield back my time.

I recognize Ms. Johnson for her five minutes.

Ms. JOHNSON. Thank you very much.

You know, apparently we are doing a pretty good job since we have not faced any real disaster since 2001, but I still am very concerned about the behavioral science because like Mr. Hall, much of my experience has been in airports, and there are times when I see people who look the least interested or able to be a threat—or just sometimes irritated to death by TSA. So, I wonder whether or not there is some training that would give the skills or encourage or at least alert, the employees of the skills to look for behaviorally.

There are times when—we travel very often, weekly, going back and forth, and many times we know, we get to know the people who are there, and yet there is still an overabundance of checking, and they have tried many times to do alternative ways for frequent travelers and what have you, and I guess what I need to understand is, what technologies or skill bases are being used to detect behavioral changes, or observations that can go along with the technology that would put a little bit of common sense in some of it.

Dr. PEURRUNG. Well, what I would say in response to that question, Ranking Member Johnson, is that it has long been known that the skill of the operators of the technology and the skill of the many professionals that are involved in security operations in airports and other venues must be a critical part of any technology system. They must be engaged in a technology development process. At the end of the day, the technology is valuable but it is their human skill. I am agreeing with you that it has to be integrated with that system. That has been known for a long time. I am not sure other than that that I have a specific answer to your question.

Ms. JOHNSON. Thank you.

Dr. Peterson, in your testimony that you submitted, you mentioned that the National Science Foundation award to the University of Texas at Dallas on the substantive expertise, strategic analysis and behavioral foundations of terrorism, and you gave heard my previous question. I would like to know what might be the expectations or what directions are you expecting of that research?

Dr. PETERSON. Well, I think I probably couldn't comment very specifically on exactly that particular program in terms of the details but I can say, as I mentioned in my testimony, that it is quite clear that these kinds of challenges involve not only scientific and engineering challenges but clear issues related to social, behavioral and economic sciences. One of the advantages that I think we have at the National Science Foundation is the ability to reach in and to establish and encourage and support partnerships across not only the technical areas, the science and the engineering areas but the social science and behavioral science areas. The one example that you have of how engineers and scientists have collaborated with the social sciences working in this.

So obviously, we don't have, you know, a whole lot of direct expertise at the back end of these processes, that is, knowing exactly the specifics of TSA protocols and so forth, but I think we are conducting a fair amount of research at the front end to understand more clearly how the social aspects play a role in the scientific and technical aspects as well.

Ms. JOHNSON. Thank you very much.

I yield back, Mr. Chairman.

Chairman HALL. The gentlelady yields back.

I recognize Ms. Biggert, the gentlelady from Illinois, for five minutes, and thank you, Madam, for staying within your five minutes.

Mrs. BIGGERT. Thank you, Mr. Chairman.

Dr. Peurrung, how are the National Labs supporting industry advancements in threat detection?

Dr. PEURRUNG. The National Labs are a resource to industry. We are a partner to industry. There are times when industry—there are many times when industry is the absolutely, you know, central role in developing threat detection technology but there may be operational capabilities that they may lack. There may be sort of scientific or technological breadth that they may lack so there are many times when a partnership between a laboratory and industry is warranted. The laboratories have no interest in competing with industry, no interest in manufacturing things as a general rule, and therefore, you know, as the technologies mature, we often start looking to industry, American industry, as a way to hand that off and make that a win. Also, industry can provide the sustaining capability in the long run, again, as I said in my testimony, to ensure impact.

Mrs. BIGGERT. Do the industries—or how often do they come to you to conduct work for them, or vice versa, how many times do you go to the industry?

Dr. PEURRUNG. It is a fairly frequent thing both ways.

Mrs. BIGGERT. Then Dr. Gowadia, it seems like a lot of the Domestic Nuclear Detection Office work is coordinated with other nations. How does the U.S. research and development in nuclear threat detection compare to other nations?

Dr. GOWADIA. I have to say we take the lead on a lot of things. For instance, in the Global Initiative to Counter Nuclear Terrorism, which is a partnership between the United States and Russia, we certainly lead the efforts to provide national architectures, to provide best practices for nation-states to provide their own—to develop and implement their own capabilities and strengths, not just through the detection mission but also in the nuclear technical forensics mission.

Mrs. BIGGERT. Thank you.

Then just for anybody, how is the facial recognition technology being integrated into the threat detection, if at all? Is that being used?

Dr. PETERSON. Maybe I could just give one very quick example.

Mrs. BIGGERT. Dr. Peterson, yes.

Dr. PETERSON. And this is also related to the question of interacting with industry. We have a number of programs within the Foundation that are center programs that involve collaborations not only with universities but also with industry. One example of one of our industry-university cooperative research centers, which is housed at West Virginia University, looks at biometric systems trying to address and focus on this particular issue that you are asking about. That is just one example of universities and industry working together.

Mrs. BIGGERT. Thank you.

Then research and development seems to be so important to everyone, and I think there are a lot of collaborative projects going on, but is there something that is unique contribution to the threat detection research and development in your agency? Maybe Dr. Cavanagh, is it something unique?

Dr. CAVANAGH. We have been involved in developing a strategy for the standards that are needed across the board but we don't do that in isolation. We do that very closely with other agencies. I don't think within our agency we have a standalone program to speak to.

Ms. BIGGERT. Is there anybody that does?

Dr. GOWADIA. I guess the Domestic Nuclear Detection Office actually is a rather unique construct insofar as we have a singular focus on the nuclear threat and we integrate efforts not just in research and development but all the way from the planning and the strategic, research, development, test and evaluation, putting detectors in the field, supporting the detectors once they are in the field. So we do have this unique larger breadth that makes sure that the research and development is well balanced and we don't sacrifice future for present.

Mrs. BIGGERT. Going back to our work with Russia, and certainly there is always—there has been right now to reduce all of the nuclear weapons in both countries and to do that. Does that have anything to do with the detection?

Dr. PEURRUNG. Well, that effort is part of the overall multi-layered approach to global security. If you can catch the material at its origin, that is one of the easiest steps in the overall process.

Mrs. BIGGERT. Thank you very much.

I yield back.

Chairman HALL. I thank you.

And the Chair now recognizes the gentlelady from Maryland, Ms. Edwards, for around five minutes.

Ms. EDWARDS. Thank you, Mr. Chairman, and thank you very much to our witnesses.

I mean, I do think, as the Chairman and Ranking Member have indicated, the challenges that we face—and we keep describing it as a post-9/11 world but this is actually just the world that we are going to live in—and that we have lived in, and, you know, they are unique and they are great. But it does seem to me that even, you know, looking at the news of the tragedy in Bulgaria yesterday, that the threats are always changing, there are new methods that are being employed, and a lot of what we see currently is not sort of the high-tech stuff, it is the low-tech stuff. It involves behavior and analyzing human behavior and looking at the dynamics of, you know, sort of culture and people and those sort of things. And yet in this environment of budget constraints, it seems that a lot of our resources, because it is expensive, goes to the nature of the really big threats that are high-tech, that require a lot more sophistication in terms of research and analysis. And so I wonder how you prioritize in this kind of constrained fiscal environment, where you place emphasis in terms of research. I think about the Center of Excellence at the University of Maryland and the START program—which I think is really, you know, a useful way to begin to analyze some of the, you know, globally what is happening on that more behavioral human front—but it is not, you know, it requires obviously high-tech data and research, but it is looking at a whole bunch of things that are not the kind of nuclear and chemical and biological threats that we have spent a lot of time today talking about.

And so I wonder, particularly from NIST and DHS, if you can give us a sense of what you can do with constrained budgets to place priorities where we see most of the threat.

Dr. GOWADIA. If it is okay, we will go with DHS first on that answer. When it comes to the behavioral aspects, at DNDO in particular, we are beginning to look at deterrents theory and analysis. And this is one of the projects that we would have liked to work with our partners at NSF this year, but had to be delayed on account of some of the budget cuts until next year.

But I would like to draw you back to something I mentioned in my oral testimony is—we do not look at this problem singularly from the lens of technology. It is close coupled to intelligence information and law enforcement skills. So we are able to bring our detectors to bear, search for nuclear material and weapons—when we have credible information. We are able to leverage not just the technology element, but knowing that the intelligence community will give us some information. And I cannot stress the invaluable law enforcement skills that are honed day in and day out in our partners.

Dr. CAVANAGH. From a NIST perspective, most of what we bring is measurement science and physical standards and calibrations, and when we get guidance from an agency like DNDO—where there is a need for such metrology support—touching into the social sciences I think we would be responsive but we are not in a very good position to take a lead on that.

Ms. EDWARDS. Hasn't DNDO faced about 38 percent in cuts from last fiscal year to the current fiscal year? I mean, I don't know what you do when your budget is cut 38 percent and you are supposed to figure out how to do all of this research.

Dr. GOWADIA. Well, one of the things we tried to do was to sort of stretch out and bridge programs as best we could. The President's 2013 budget request does try to restore our research and development portfolio back to a healthy level. We took actually the predominant cut in our long-term research program, and so again, one of our extremely powerful programs, our academic research initiative, bore some of the brunt and we had to diminish our ability to support students, almost 40 of them this year. That was hard.

Ms. EDWARDS. Well, I hope we are going to take a look at the vulnerability that we put ourselves in when we make cuts like that—that tend to be across the board but actually go to the thing that will most enable us to analyze threats, detect them, and prevent them in the future, and with that, I yield.

Chairman HALL. I thank the gentlelady, and I recognize the gentleman from Illinois, Mr. Hultgren, for five minutes.

Mr. HULTGREN. Thank you so much. Thank you all for being here too. I really appreciate the work that you are doing. This is a very important topic for us to be discussing, and I think it is a really important intersection as well for us to be talking about how science is important to our safety right now, so thank you so much.

A couple questions I have just to see if any of you have any thoughts on this. But I wonder how the technologies we are discussing today work within the wider systems approach to protecting the public from dangerous materials, and I wonder also how are the technology end-users and screeners involved in the development processes?

Dr. PEURRUNG. So when a question comes up about how the technologies work in the wider system perspective, that makes me think of again the point that mission-user input, early in the process mission-user engagement is absolutely critical. Of course, they should be setting the requirements, but beyond that, they should be providing feedback to the technology developers and the scientists at every stage of the process, if possible, because all too many good technologies struggle when it comes to the point of being deployed into the field.

Early in my career when I was a researcher, I learned early on that a technology in the field could have two, maybe three lights on it. It could have a red light, fail; it could have a green light, pass; and maybe a yellow light to say something else is wrong with the system, and that is a real shock to a Ph.D. researcher who has come out of school and is used to hundreds of knobs and dials. So that is an important thing to get right from the beginning.

Dr. GOWADIA. Well, at DNDO, sir, we have what we call our solution development process, and it is a rather rigorous process that brings the operators in, as Dr. Peurrung just mentioned, early on to help define not just the mission need but the early requirements, et cetera. We use their input all the way through. They are part of the test program. In fact, they are beginning to move further and further down into our science elements now where advanced technology demonstrations, we are bringing the users in, getting feedback and doing more research before we advance the technologies so we know that we are putting technology out that will meet their needs and building collaboration with them.

Mr. HULTGREN. Can you give us something a little bit more specific? And the Chairman referenced the travel that we all do and we are back and forth every single week pretty much out here, and one of the things I have seen both here in DC. and even earlier in O'Hare where I travel through is the expansion of the whole-body imaging systems that they are using, and I just personally feel a little uncomfortable with that. It struck me, my wife and I traveled recently, and I felt very uncomfortable of having my wife go through that. I hear from other people as well, just some privacy concerns, and I feel like this is an ongoing challenge that we have is, we have got technology but we also have a commitment to privacy and respecting privacy. On top of that as well is just safety—these are X-rays still and if you are going through every single week, a couple times a week, I know it is very small impact but if there is susceptibility to some of that radiation, is there a problem there? So I guess I would just ask you quickly if you could talk a little bit more about this technology. Do you feel like the privacy concerns have been adequately addressed, or could more be done to ease these concerns so that we are doing everything we can to have safety but at the same time protect privacy?

Dr. PEURRUNG. I don't know that I can personally offer anything on finding the right balance between privacy concerns and security concerns. As the technology developers, unsurprisingly, our goal is to deliver the best possible system from a technical point of view, and we did that, and before 9/11 there were actually foreign deployments of that system by other governments who had far less concern for privacy. After 9/11, of course, the equation changed, but I agree with the premise of your question which is that privacy is a significant issue. There certainly are ways to address it but finding that right balance is, I am afraid, not appropriate for a national laboratory to comment on.

Dr. GOWADIA. Again, this is really for TSA and Science and Technology to respond to, so I apologize, sir. I don't have a clear answer for you today.

Mr. HULTGREN. I think one of our challenges is getting answers from TSA as well and having them be a part of our discussions. I am pleased to serve on this Committee. I also serve on the Transportation Committee and the Aviation Subcommittee, and it has been one of our great frustrations is to try and have them be a part of this discussion so we can make plans. So I know the Chairman has been frustrated with that and the chairman of the Transportation Committee has been frustrated as well. So these are important. I understand and respect your point of view as well, that your charge is to create the best technology available. It is really our responsibility to be that balancing agent, and when we don't have all the information, it is very, very difficult for us to do our job there of protecting those previously concerns and security concerns and struggling to find that balance. So I hope TSA will be more engaged in this process and be more helpful.

My time is up. Chairman, thank you so much. I yield back.

Chairman HALL. And I thank you.

The Chair recognizes Mr. McNerney from California for five minutes.

Mr. MCNERNEY. Thank you, Mr. Chairman.

Mr. Peurrung, about helium-3, I would just like to get a basic idea how that works. Does the gamma radiation make that nucleus unstable, which is easy to detect?

Dr. PEURRUNG. So a helium-3 neutron detector works because the neutron, once it has been slowed by a process called moderation, interacts with that helium-3 nucleus. It has an exceptionally high propensity to have that interaction. That is why helium-3 is special. And that releases a large amount of energy that can be deposited in a very short spatial distance. That is a unique thing, and that is how a helium-3 tube, we call it, works. There are alternate technologies as we, both Dr. Gowadia and I, described in our testimony, that work through fundamentally the same physics. They just use different materials that are non-gaseous. Helium-3 is a gas, which is why it was along with something called a boron trifluoride tube that some of the earliest technologies in neutron detection.

Mr. MCNERNEY. Thank you.

Dr. Cavanagh, would you discuss the state of standards for nuclear threat detection? Where are we with the creation of the standards for the equipment or testing?

Dr. CAVANAGH. In terms of testing for nuclear materials, we have worked with DNDO to set up something like the National Voluntary Laboratory Accreditation Program so industry and detector providers for nuclear detectors can have those detectors evaluated and their performance ascertained by an independent party. So some of that is documentary standards. Some of those are calibration standards. Some of those are performance standards.

Mr. MCNERNEY. Are standards being developed now for testing or equipment for nuclear threat detection?

Dr. CAVANAGH. Some of the standards that are in place are public standards. Some of the standards are more sensitive and they are still being developed to be more specific in terms of requirements.

Mr. MCNERNEY. Thank you.

Dr. Gowadia, how imminent is the nuclear terrorist threat in this country?

Dr. GOWADIA. That is a hard question to answer directly. What I will tell you is, we look at the threat from start to finish. So we look the availability of materials, terrorist-expressed intent, couple that with expertise from the National Labs and what they know about how those materials can be fashioned into a weapon or a more imminent threat, and then we analyze our architecture all the way from source to target and see what capabilities we have defensively along the way. That allows us to prioritize our efforts and drives our mission. So it is a risk-based approach that we take based on all we hear from the intelligence community and from the science world.

Mr. McNERNEY. So how—what kind of cooperation are we getting from our international partners? I mean, it seems the best place to stop a nuclear device from entering our port is to stop it before it leaves the port of origin. Are we having a good amount of cooperation with other nations in terms of developing techniques to make that a reality?

Dr. GOWADIA. So we do work within not just the IAEA construct, but also the State Department—the global initiative construct—to actually work with nation-states to begin to give them best practices on securing their materials. So we are further back in the chain, not just starting at the ports. We look right where the material is. And the DOE certainly—and Dr. Peurrung could probably speak to this—has a lot of programs overseas that look at essentially the first line of defense on how can the material not leave the foreign nations on its way here.

Mr. McNERNEY. Are we getting good cooperation from those nations?

Dr. GOWADIA. In the global initiative, yes, we are. We have—and the IAEA in particular—has been rather a champion of our best practices.

Mr. McNERNEY. Dr. Peurrung?

Dr. PEURRUNG. Yeah, my laboratory worked in over 110 countries in a recent fiscal year and that is largely the result of NNSA international—we call them international deployment programs—and I would say yes. Of course there are degrees to this, but there is a lot of great cooperation from our international partners.

Mr. McNERNEY. Thank you.

Dr. Peterson, one last question. Do you believe that the federal agencies are using research findings as they become available, or is there a huge lag in deploying technology that is known from academic research?

Dr. PETERSON. Well, I think there are certainly opportunities to better the so-called lab-to-marketplace transition, and as you probably know, there are new programs at the National Science Foundation and in other federal agencies that are trying to address that particular issue. I do think it is important in this issue, as well as others, to have strong research ties to industry and to not only develop what people would call applied research portfolios based on that, but also to have their basic research and fundamental research activities be integrated and tied to potential applications. So I think we have tried to address those issues in different ways and I do think it is important, yes.

Mr. McNERNEY. Thank you. Mr. Chairman, I yield back.

Chairman HALL. And I thank you and I recognize Dr. Cravaack from Minnesota, five minutes.

Mr. CRAVAACK. I think that is above my pay grade, sir, but I will take it. Thank you.

Thank you to a very distinguished panel for being here today. I appreciate all that you are doing, and I have just a small smidgen of probably what you are talking about, so I appreciate everything that you are doing for us. But one of the things I do know a little bit about is education, and Dr. Gowadia, in referencing your testimony, it is obvious the types of research that you perform in the division of mathematical sciences necessitates a strong STEM educational background with people that you work with. Do you find that you have enough qualified STEM-educated Americans to produce the types of mathematical research, algorithms, statistical methodology to develop the new threat technologies that you are speaking about?

Dr. GOWADIA. Thank you, Congressman. Yes, actually we have two programs at DNDO specifically addressing ensuring this expertise pipeline for the United States government at large. The first is the Academic Research Initiative, which you have heard Dr. Peterson speak about, and the second is a congressionally-mandated program where we look at the forensics expertise pipeline close coupled with the laboratories. There we are setting up these career paths for these young engineers and scientists so that we can retain that expertise and have it brought to bear on our mission.

Mr. CRAVAACK. How deep do you reach down? What age groups are you talking about here?

Dr. GOWADIA. We go all the way to undergraduates, all the way to the graduate system, postdocs, even professors. We support their efforts.

When we select our proposals, sir, we make sure that it is not just—it has technical merit but also we look at the coupling of, are they supporting enough students.

Mr. CRAVAACK. Thank you.

Dr. Peterson, it is my belief that we should reach even further down than that. I mean, we need to capture these kids early on and get them hooked on science, so to speak. What is your opinion on that?

Dr. PETERSON. Absolutely, and let me just say a little bit more about this, the program that we have in partnership with DNDO. The proposals that are submitted for this partnership are submitted to the National Science Foundation and are reviewed by the NSF merit review process, and it looks not only at the technical merit of the proposals but also at what we call broader impacts. That does specifically have to do with one's ability to articulate how important that research is in other areas, not just to the researchers that are actually conducting the work. And many faculty members and students in universities do that through interaction with pre-college opportunities, whether they be middle schools, elementary schools and so forth. So while we don't have a very specific program that is designed just explicitly to do that through this DNDO partnership, I would say that many of the research projects that we do support in this partnership have educational components that reach into the pre-college arena.

Mr. CRAVAACK. I think it is vital. One of the things that I think that we need to do, and I agree with one of my colleagues that just spoke about this, is we have to have a renewed emphasis on STEM in our country. Dr. Peurrung, did you want to comment?

Dr. PEURRUNG. I would just agree strongly with your comment, and the laboratories in general also have a role to play here. Battelle, that operates our laboratory, have played a critical role in standing up a STEM-based high school in Richland that we hope is a model and also in working to reform the science and math curriculum with the partnership of the State of Washington.

Mr. CRAVAACK. I think it is vital. It is my hope that we continue to develop STEM-type of initiatives like the National Flight Academy down in Pensacola, Florida, spending time on a simulated aircraft carrier to get kids hooked on what it takes to fly an airplane or, you know, what it takes to navigate a ship or build a ship and the technologies associated with it.

So I truly believe that capturing these kids early on where it is cool to be an engineer, it is cool to be a scientist and how much we value science and technology in this country. So I think it is one of the major—the kids hold the future, and we want to make sure they are part of that.

Dr. Cavanagh, it seems like you want to say something.

Dr. CAVANAGH. NIST also is very much engaged in STEM. We have had roughly 175 students over each summer at NIST. We also have—in terms of reaching down, we also have a small program for middle-school teachers, science teachers to bring them and engage them with what is currently going on.

Mr. CRAVAACK. You hit the nail on the head. Not only is it important that we educate, you know, our children but we also have to get those great teachers, those fantastic teachers that can turn some young kid interested into the mathematics and sciences of this great country of ours.

So thank you very much for that comment, and it looks like my time is up. It was a good subject, though. Thank you for your comments, and I yield back.

Chairman HALL. I thank you.

The Chair recognizes Ms. Bonamici, the gentlelady from Oregon, for five minutes.

Ms. BONAMICI. Thank you very much, Mr. Chairman, and thank you all for your testimony and certainly for all the work that you do to protect our national security.

Dr. Peurrung, you mentioned that the Pacific Northwest National Laboratory was the first to detect trace amounts of radioactive material over a U.S. territory after the Fukushima tragedy. As someone who represents part of the Pacific Northwest coast, I thank you for your work. I am asked on a regular basis if there is radioactive materials in the tsunami debris that is washing up on the shore, so let us work together on that.

You also said in your testimony that approximately half of your business is centered on national security missions. Can you—I know there has been some talk about budget cuts. Can you talk a little bit about how your laboratory has been impacted, if at all, by recent cuts to the DHS Science and Technology Directorate?

Dr. PEURRUNG. Well, the cuts to the DHS Science and Technology Directorate are part—you know, that is one of our many diverse markets—and certainly those cuts were significant. My goal as a steward of capabilities of the national lab is to manage through these fluctuations in funding in a way that preserves the maximum amount of critical capability. We have been largely able to do that. One of the main reasons for that is that the capabilities that are funded by DHS S&T would be things like chem and bio detection, cyber infrastructure protection, things like that, that are also—as I made the case in my testimony with any strong research program—funded by a range of other federal sponsors. So at the moment, there has really been what I would call moderate impact. As with many DOE labs, we have had some reduction in staffing, but really the capability preservation has been fairly successful to this point.

That said, one more quick point. I think that the concern going forward is again about strategic stewardship and whether—in this era of budget cuts—whether there will be excessive focus on the threat of the day or short-term objectives.

Ms. BONAMICI. Thank you very much.

And I know that many of the technologies that you all invest resources in will be used by state and local law enforcement and first responders, and there is of course a lot of variation. What New York City needs may be very different from what Cannon Beach, Oregon, needs. We had in Oregon a few years ago TOPOFF 4, that was a simulated detonation of a radiological dispersal device. Thousands of people participated in that exercise, and part of that goal was to figure out the communication needs with local responders.

So knowing that you are all engaged with Department of Homeland Security Science and Technology Directorate in setting priorities, would you please talk about the current status of coordination with state and local stakeholders in determining that your research is lining up with their needs. Especially given the budget difficulties, how will you improve engagement with the state and local stakeholders to make sure that the research is aimed at meeting their threat detection needs and requirements? Thank you.

Dr. GOWADIA. Well, I can speak to the Domestic Nuclear Detection Office, not to the S&T Directorate. But for us, our state and local partners are absolutely critical to what we do. Again, I go back to that triad. I hate to beat my triad to death but we can't do what we do without their law enforcement skills and their willingness to accept our mission. So we work very closely with them on individual bases. We go out into the states and work all the way from the governor's office down into the highway patrol.

I will give you a good example. Very early in DNDO's life, we had a small program called the Southeast Transportation Corridor Pilot, and Florida was one of the key partners there. We started working with them early on, and Florida, of their own accord, has now statewide rad-nuke detection enterprise. So we worked with them on training, the detection technologies they need. They have shaped the development of our new hand-held system by actively engaging with us. Once they have alarms in the field, we support them with the alarm resolution. We have a joint analysis center that takes calls from the field and works with the National Laboratories to give them advice on how to respond to the alarm and deal with it.

And one other unique thing we have is our red team. So, very often the state and local partners will call the red team in to test themselves in the operational world and keep building and growing. When DNDO started, I don't think half the country had rad-nuke detection systems, but today more than half of it does.

Mr. BONAMICI. Thank you very much. Anyone else in connection with local and state?

Dr. PEURRUNG. Well, we consider them to be again critical mission users. We have an office in Seattle that is particularly engaged with us, Northwest Region First Responders, and in the interest of time, I will cut it there, but they are critical mission users that we must collaborate with.

Mr. BONAMICI. Thank you very much.

My time is expired. Thank you, Mr. Chair.

Chairman HALL. I thank you for yielding.

Congressman Benishek of the State of Michigan for five minutes, sir.

Mr. BENISHEK. Thank you, Mr. Chairman, and thanks, members of the panel. I really appreciate your being here. This is an interesting subject.

I have a border district in northern Michigan, okay, and we have, you know, a bridge to Canada and we have a river that, you know, provides a border, and you know, I am concerned about the threat across—somebody taking a boat across the river. Is there any new technology, you know, other than just patrolling the river that is available, you know, on bridges or on rivers that would protect my district any better than just the patrol boat? Can you enlighten me about that?

Dr. GOWADIA. Well, sir, we have actually been working on the water detection at DNDO, and we found some promising capabilities for some standoff detection from a small boat to a small boat, so we are beginning to invest a little bit further in some of those technologies. What I will assure you is that all Coast Guard boarding parties have rad-nuke detection equipment, so when a Coast Guard vessel is available, they will bring that capability with them, so you already do have some coverage by way of your Coast Guard.

Mr. BENISHEK. Let me ask another question. What is the most—what are the things that you are most worried about and what is your highest threat from your point of view? Any one of you if you have a comment but I am thinking of Dr. Gowadia since you are with, you know, the radiation agency.

Mr. GOWADIA. Right. So sir, we actually look at the global nuclear detection architecture rather holistically. We try to balance capability in all pathways so that there is something in the air domain, something in the land domain, and certainly something in the maritime domain. That is how we try to make sure that there is as much capability put in place for defensive measures against an adversary across the pathways.

Mr. BENISHEK. But there is not like one single thing that you think is the most serious threat? I mean, in your own mind.

Dr. GOWADIA. Those are some thoughts. Perhaps we can take it to a closed room, sir.

Mr. BENISHEK. All right. I understand.

Dr. Peterson, you know, as a scientist myself, you know, I see that this whole process must be bringing in tons of data from, you know, all kinds of different sources, and it is of some concern to me, you know, how do you—what is your process for, you know, collating this data, making it translate into policy? I mean, what is the timeline for that and what is the process?

Dr. PETERSON. That is a great question, and it is applicable not only to this particular problem but to many other areas of research right now. The whole issue of so-called “big data” and how do you deal with it, how do you best process it, mine it, store it, make it accessible not only to the researchers that collected it but to others. How do you make it one set of data as easily accessible as another set so that one can look at integrated sets. What I can say is that the NSF is investing a fairly significant amount of money. Big data is part of what we—you know, we love acronyms. There is a cross-foundational program called CIF21. And this year, NSF in partnership with other agencies launched a very specific focus on how best to handle these large amounts of data and do the analyses that we described. So I can’t give you a specific example for this particular problem, but it is certainly an issue that we are trying to engage the academic community in researching.

Mr. BENISHEK. Dr. Peurrung, do you have a thought?

Dr. PEURRUNG. Yeah, I would—I think it is useful to break the challenge into three parts. I think they are all the subject of a great deal of ongoing research. The first is, we need new software tools that can make sense of the data, combine different types of data, handle data volumes and streams. The second is, we need computing architectures that can cope in a reasonable time frame with the mind-boggling amounts of data that are sometimes available. And the third is, you need analytical environments and visualization tools so that the human-computer interface gets to be more effective. So there is sort of in my mind three fundamental challenges there.

Mr. BENISHEK. Do you have somebody scanning like private-sector innovation and other government things? Do you have somebody doing that on a daily basis, or how does that work?

Dr. PEURRUNG. This is one of those areas where we are already in various collaborations with industry around this.

Mr. BENISHEK. At the end here, I have one more question. You know, this bridge I am talking about, you know, since 9/11, the traffic on it is so slow because of the risk and the commerce that we have in northern Michigan across that bridge has really changed due to the delays and everything. I understand the increased risk of the security but the commerce is definitely suffering for that, and is there ways that that can be, you know, expedited? Is there any thoughts on that? Is there any work on that trying to expedite the flow of traffic on our border crossings to, you know, aid commerce?

Dr. GOWADIA. Well, Congressman, I do know that in everything we deploy from a security perspective, we do keep in mind the flow of commerce and try very hard not to impact it. Not knowing exactly what is impacting that bridge, I feel at a little bit of a loss to help you with that. But we do consider the flow of commerce in all our studies.

Mr. BENISHEK. All right. I guess my time is up. Thank you, Mr. Chairman.

Chairman HALL. And I thank you.

The Chair now recognizes Mr. Luján, the gentleman from New Mexico.

Mr. LUJÁN. Thank you, Mr. Chairman, and I appreciate the panel very much.

The conversation about access to STEM for our students, I appreciate that conversation, and I think it is an area we need to highlight. Dr. Gowadia, I believe you talked about 40 interns that you weren't able to bring on or that you had to let go because of budget cuts. We need to be cognizant of that. As we talk about the need for more scientists, physicists and experts in our fields, we have to understand that there is impacts with budgetary cuts. And with that, what has been the effect of the budget cuts? Have we lost research teams or infrastructure that will be difficult or expensive to reconstitute?

Dr. GOWADIA. Congressman, fortunately this just been the first year, and I do hope that the President's budget request—where we tried to bring our scientists back to a healthy line—is given favorable consideration. Fortunately, since this is the first year, we have done everything possible to either extend periods of performance, keep people going as long as possible, and it hasn't come down to infrastructure loss yet. But the cuts have impacted some of—for instance, we were not able to give any new grants out at all this year in the Academic Research Initiative. Of the 32 grants we had, we have held 13 at 100 percent funding, or high-priority ones, and the others are at about 50 to 60 percent funding, which is why we had to drop 40 undergraduates this year.

Mr. LUJAN. I appreciate that, and with emphasis on impact to infrastructure yet. I think we need to be very aware of that as well.

I am going to ask a line of questions that maybe we don't talk about enough, and I am intrigued to find out how it impacts what we are looking at when it comes to detection of fissile material coming into the United States of those that may want to do harm to our homeland. I am sure that you studied behavior, organizational structure, trafficking patterns, areas of vulnerability to the United States. You highlighted an example of how you worked with Florida from the top down all the way to law enforcement on the ground, and we understand how these items may move.

I am extremely concerned that we still can't stop narcotics from moving into the United States. It is clear that when the Department of Homeland Security was created, and we look back to 2004, the counter narcotics enforcement program was created in 2004 by the Intelligence Reform and Terrorism Prevention Act. I think we saw then and we know now that there are very much tied to one another. We constantly detect tunnels that are being closed. We know now that there are submarines that are not able to be detected by some of our radar capacity that are moving in large amounts and volumes of narcotics as well. What are we doing to take advantage or to employ technologies to better understand behavior where the United States has serious risks, serious threats—narcoterrorism cells that have been tied by the intelligence community as well as the Department of Homeland Security—to make sure we are stopping that activity so that way we can better police what is happening with areas of vulnerability with fissile material potentially entering the country? And I would open that to anyone.

Dr. GOWADIA. Again, sir, we look at the nuclear threat, again not just from the pure technology element, but intelligence-informed searches and surges. So in moving our architecture and our architectural strategy away from the notion of serendipitous encounter with larger detectors——

Mr. LUJÁN. Well, if I may, I apologize but time is running out, I am not talking about serendipitous encounters associated with narcotic flows. When I look at DNDO, they work to determine gaps and vulnerabilities in the existing global nuclear detection architecture and formal recommendations and plans to develop enhanced architecture. DNDO also conducts, in accordance with a long-term research and development program to address, that complements what is happening with the Department of Energy. I think Pacific Northwest Laboratory highlights the work they do for DHS in addition to DOE and NNSA, as far as the intelligence community. From a science perspective, the NSTC Committee on Homeland and National Security provides guidance and direction to the NSTC to increase the overall effectiveness and productivity of federal R&D efforts in the area of science and technology related to homeland and national security. All I am suggesting is, if the stuff is going to move in, we know where the dollars are going to support these terrorist cells. It is not a big secret.

And, you know, I have other questions pertaining to helium-3. I am extremely concerned associated with the shortages that we have and how we can work with the National Labs, and we will submit those into the record. All I am asking is, as we talk with the experts and some of the smartest people that we have—which many of them are right in front of us and those that you work with—talking about data, computing, the analytical responsibilities that we have as a country. There is a big threat to our Nation, and I am suggesting that if we can't stop this other stuff from entering the homeland, it only opens us to more danger with what could happen with these other cells looking to exploit these narco-terrorists, cartels from doing bad.

And with that, Mr. Chairman, I appreciate the indulgence there and yield back my time. But I thank the panel very much.

Chairman HALL. And I thank the gentleman. He asked good questions.

I am honored to recognize Mr. Rohrabacher for five minutes, the gentleman from California.

Mr. ROHRABACHER. Well, thank you very much, Mr. Chairman, and I apologize. We have two hearings at exactly the same time. They are both very important, and so I am coming a little late to this one.

I can't help but notice that when we talk about budget cuts, in fact, the Department of Homeland Security has had budget increases overall. I am not talking about necessarily your departments but there hasn't been a major budget cut. It has gone from $55 million to 59, is it billion or million? Billion. Fifty-five billion to $59 billion. And so when my colleagues mention the budget cuts even under this Administration, I don't—someone within the system then has prioritized. If you are receiving less money for technology development, they prioritize even in an expanding budget to decrease your own, or maybe what is happening is, Mr. Chairman, perhaps people are talking about a reduction in the increase, which is a game that we have heard quite often over the years.

Mr. Chairman, when we expand our technological capabilities for defense, it is a double-edged sword, and the double-edged sword is, anything that can be used to protect us can also be used against us, and what are we doing to make sure that—and is there a way that we can actually increase our abilities technologically for surveillance, et cetera, without having that also being an alert to us that we have got to be more careful that our new capabilities aren't being used against honest people and to control the people rather than protect them? I am just opening that up to the panel for discussion. I guess the Department of Homeland Security.

You know, I remember when I was a kid driving to the airport, jumping out of my car. I was late for the plane. I ran from the curb to the gate. The door of the plane was closing up. The stewardess said come on in. I got in. The plane took off and the stewardess took my ticket on the airplane. We can't do that anymore. Here we are, we are very protected now. I get patted down. I have to stand there with my hands in the air. We are doing all of these things to protect us but I have to tell you, my freedom as an individual American has been dramatically impacted to the negative because of what we have done to protect us against perhaps a worse negative, which would be a terrorist attack. And I might add, in that very same airport that I did that, there was a bomb that exploded, and later on as a reporter, I covered this bomb explosion and I saw where people's shoes were there and their legs had been blown off and their feet were still in their shoes.

So this is—every comment and everything we do I guess has a flip side. What are we doing to make sure—what are your views on the technology development and how we are going to make sure it is being used for protection, for benefit rather than against our freedom?

Dr. PEURRUNG. Well, a comment I would make to your question is simply that a researcher who works on threat detection technology should bear in mind the many technical challenges. They want faster measurements. They want more sensitivity, more background rejection abilities, see-through shielding, all of these things that we all know and understand but operational impact and operational suitability have to be high on that list of parameters that matter, and I believe that is recognized by the research community.

Mr. ROHRABACHER. Thank you very much. That was a very good answer.

Mr. Chairman, I yield back.

Chairman HALL. I thank you for yielding.

The Chair now recognizes the gentleman from Illinois, Mr. Lipinski, for five minutes.

Mr. LIPINSKI. Thank you, Mr. Chairman. Thank you for holding this hearing today.

Chairman HALL. I hope Rohrabacher hasn't scared you to death.

Mr. LIPINSKI. I have learned to ignore Mr. Rohrabacher sometimes.

I think this is critically important. As Mr. Rohrabacher very clearly illustrated the dangers we are facing, I think it is easy for some to forget or not understand how important the R&D is to help keep us safe from the threats that we are facing and the ever-changing threats that we are facing.

I just wanted to briefly first mention something, talk about something that has been brought up by a number of Members here today. I am also concerned about in recent years the cuts that DHS has had in its R&D budget, especially the 38 percent drop in funding between fiscal year 2010 and 2012 to the research, development, acquisitions and operations account. I know at Argonne National Lab outside Chicago, there are a number of research projects for the Department of Homeland Security that are going on, including risk analyses of risks to our critical infrastructure and the development of sensor technologies to help detect threats. These are the types of things I believe we need to be doing, and I hope that we in Congress make sure that we are providing the funding that is needed for this part of our defense from the threats that we are facing. I know a lot of my colleagues have mentioned that. I just wanted to echo that.

The question I wanted to raise has to do with the social and behavioral sciences. As someone who was in that field, after being an engineer, I just—I understand how critically important social and behavioral sciences can be in terrorist threat detection. They help us understand what causes a person to turn to terrorism, who is likely to try to attack us, and by what means. For example, I mentioned Argonne National Lab before. I know that they are conducting research in Asian-based social network modeling to investigate possible terrorist networks. Now, due to our budget situation, however, and I think to some extent a misunderstanding by some of what the social and behavioral sciences can teach us, there has been a suggestion that we should cut back on funding for social science research. So I would like to hear from all of our witnesses, whoever wants to jump in on this, how your agencies and labs are using social and behavioral science research to aid in your efforts to improve terrorist threat detection. Whoever wants to start. Dr. Peterson?

Dr. PETERSON. Congressman Lipinski, thanks for giving me a chance to respond to that. I have already made comments about this before, but let me just reiterate the primary point, and that is, I think, that we cannot contribute substantially to this particular issue, and many other grand challenge issues that this country and the world faces, without close partnership among the physical sciences, engineering, the life sciences and the social, behavioral and economic sciences and education. And I think we have demonstrated how important the Foundation feels this is by the emphasis we are placing in many cross-foundational programs that require partnerships among the disciplines that I just described. This is a very good example of this particular issue with respect to threat detection technologies of how important it is to have the influence and the expertise of the social, behavioral and economic sciences.

It is sometimes a challenge to engage these strongly interdisciplinary communities in focusing on these kinds of research problems. It is a challenge, first of all, to encourage individuals who may be focusing on more theoretical aspects to understand the richness of the basic research that still is involved in some of these more applied issues. It is a challenge to make sure that the language that the engineers and scientists use can be understood by the social scientists and vice versa. I think it is most important, again from the NSF perspective, it is a challenge, to make sure that the social, behavioral and economic science community themselves defines the important research agendas. It is really not up to the engineers and the scientists to tell them what we need from them. It is really up to the social, behavioral and economic science community to define the important research problems that we need to focus on.

Mr. LIPINSKI. Anyone else want to—anything additional, Dr. Peurrung?

Dr. PEURRUNG. Very quickly, I concur with your point that the behavioral and social sciences are of increasing importance. We have made investments in those at PNNL, and I was really struck with a biosurveillance program, I think Georgetown University led it, I believe, that used indicators of social disruption to do biosurveillance quite successfully. That is an example.

Mr. LIPINSKI. Thank you.

Anyone else?

Dr. GOWADIA. At DNDO, we are looking at universal adversary models and things like that to begin to understand and appreciate what an adversary would need, what intent, what capabilities, et cetera, and how that would drive our systems. So we do model the adversary. We certainly have very close coupled with the intelligence community. And with our partnership with NSF, we are looking to study deterrence theory and analysis also, again, bringing some of the coupling the soft sciences with our hard-science modeling.

Mr. LIPINSKI. Thank you very much. I will yield back.

Chairman HALL. The gentleman yields back. That I suppose ends our testimony and our questions. You have been great. We really thank you and for the things you didn't tell us that you say you could tell us, Dr. Gowadia. I think we would like to hear that sometime, and thank all four of you. Thank you very much.

The Members of the Committee will have additional questions for any of you. We may send you some additional questions and ask you to respond to them in writing. The record will remain open for two weeks for additional comments from Members.

And with that, we are adjourned.

[Whereupon, at 11:43 a.m., the Committee was adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Richard Cavanagh

QUESTIONS FOR THE RECORD
THE HONORABLE RALPH HALL (R-TX)
U.S. House Committee on Science, Space, and Technology

Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies

Thursday, July 19, 2012

1. **How do your agencies stay up to speed on what other federal entities and the private sector are doing in threat detection technology? Do you have personnel dedicated to seeking out such technologies to inform agency work and to avoid potential duplication of efforts? Finally, how do you ensure that the threat detection technologies developed through federal research funding will be both economical and usable?**

Answer:

NIST relies on a variety of mechanisms to stay abreast of measurement needs in the area of threat detection technologies. Our staff participate in a variety of conferences and report back on emerging concepts where documentary and measurement standards will play a critical role in robust and reliable performance of threat detection technologies. Staff involvement in consensus standards committees insures that robust and science-based standards are available. When technologies are identified as being of interest, members of our technical staff also participate with other agency staff and the private sector in the development of strategic plans to address improvement in the performance of existing detection technologies, and the development of new technologies to meet emerging needs. For example, NIST is part of the 3He Integrated Product Team (IPT) - the Sub Interagency Policy Committee (Sub-IPC) - the Technology Working Group (TWG). This group updates the technology matrix for on-going research efforts across the US Government and identifies alternative technologies to 3He based neutron detectors.

Measurement standards are a key component in establishing the comparability of different technologies when applied to the detection of threats. Through the standards that we help develop, the community is able to determine the performance of different technologies when facing the same or different threats, such that advances pursued by one community can be readily shared with communities with different interests.

For instance, NIST is working with DHS/DNDO and DOD for testing of radiation detection instrumentation. Test equipment used as platforms for this work are based on consensus standards and standard test methods. This collaboration helps both in recognizing usable equipment and reduces cost of testing of threat detection technologies. The use of consensus standards and standard test methods also provide significant cost –savings due to their incorporation of technologies that are often already commercially available and due to the public-private partnership nature in which these products are developed.

QUESTIONS FOR THE RECORD
THE HONORABLE DAN BENISHEK (R-MI)
U.S. House Committee on Science, Space, and Technology

Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies

Thursday, July 19, 2012

1. **Dr. Gowadia's testimony mentions the inherent technical difficulties in developing nuclear detection technologies for homeland security applications (including limitations related to speed, distance, shielding, and source strength). How is NIST working to improve the ability of technologies to detect threats in challenging environments?**

Answer:

NIST is primarily involved in testing commercially available technologies and assessing the current capabilities for detection of threats in challenging environments. The challenges of speed, distance, shielding, and source strength that are inherent in nuclear detection technologies are primarily pursued by our partner agencies. NIST does have a few joint research programs with those agencies, such as one with Los Alamos National Laboratory that is looking at high resolution, compact, fieldable detectors that hold promise for impacting the ability to detect a weak source in the presence of typical background interferences. This detection approach builds on research in ultra-sensitive detectors for astronomy, and provides an example where NIST's measurement science expertise developed through the work that is consistent with the NIST mission, is being leveraged for improved threat detection technologies

QUESTIONS FOR THE RECORD
THE HONORABLE BEN LUJAN (D-NM)
U.S. House Committee on Science, Space, and Technology

Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies

Thursday, July 19, 2012

1. **It is extremely important to test threat detection technology in a realistic manner. Does the Nation have realistic test and evaluation capabilities for the threats that range from nuclear and explosive to chemical and biological? For example, do we have adequate capability to test radiation-detection gear with real threat materials such as special nuclear materials?**

Answer:

The Nation's test and evaluation capabilities for biological and chemical threat detection are agency specific, and while sharing of testing and evaluation facilities and resources are shared among Federal agencies, a robust standardized infrastructure for testing and evaluation can significantly enhance coordination of test results across the interagency community. Through implementation of the National Strategy for Chemical, Biological, Radiological, Nuclear, and Explosives Standards, led by the Office of Science and Technology Policy, the government agencies in charge of this area have initiated coordination efforts to develop national-level standards to support the needed test and evaluation infrastructure. Furthermore, validation of threat-detection technologies for surveillance and screening will most likely require extensive standards development to ascertain if technology performance is fit for purpose.

QUESTIONS FOR THE RECORD
THE HONORABLE RANDY NEUGEBAUER (R-TX)
U.S. House Committee on Science, Space, and Technology

Keeping America Secure:
The Science Supporting the Development of Threat Detection Technologies

Thursday, July 19, 2012

1. **What is unique about the development of technologies designed to detect intentional threats versus accidental threats or natural disasters?**

Answer:

Accidental threats or natural disasters are characterized by the lack of the element of human intent. In some cases the same types of instruments are used for both scenarios although deployment plans would differ.

QUESTIONS FOR THE RECORD
THE HONORABLE BEN QUALYE (R-AZ)
U.S. House Committee on Science, Space, and Technology

Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies

Thursday, July 19, 2012

1. **It seems like the National Institute of Standards and Technology (NIST) does quite a bit of work in the area of threat detection, but the work is initiated only when you are asked for help. Are there are any specific areas in which NIST is taking the lead on threat detection measurement or science? How much of NIST's work in threat detection is actually funded by other Federal agencies?**

Answer:

NIST's efforts in the threat detection area are rooted in NIST's expertise in measurements and standards, which in turn stem from the NIST mission. As a result, Federal agencies often approach NIST for specialized skills and experiences relating to measurement science and standards. Frequently, the threat detection work builds on NIST expertise in detection technologies that was funded with other objectives in mind. The measurement science of radiation detection, of particle detection, of vapor detection, and of organism detection finds dual use in threat detection and in the manufacture and use of consumer products.

2. **You state that because the National Institute of Standards and Technology's (NIST) primary mission is to support industry, NIST is frequently in a position to point to an existing detection technology that could be appropriate for detection of an emerging threat. How does NIST manage to do this in a way that isn't perceived as advantaging one company over another?**

Answer:

NIST focuses on the science behind a measurement, and assuring that different measurement methods provide consistent results when applied to the same measurement challenge. We frequently want to find two independent methods to measure the same entity, to provide assurance that the quantity being reported is independent of the measurement method used. And we are looking for agreement between independent methods to provide assurance in each method.

In the area of particulate analysis, we have developed measurement science to improve air quality; eliminate contaminant particles in semiconductor production; and to monitor engine wear. So if an emerging threat is based on particles, NIST may be able to point to detection methods that are already practiced in industry that could be applicable to the threat. The focus is on the science underlying measurement, rather than on a commercial measurement device.

Responses by Dr. Huban Gowadia

Question#:	1
Topic:	federal entities
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Ralph M. Hall
Committee:	SCIENCE (HOUSE)

Dr. Huban Gowadia

Question: How do your agencies stay up to speed on what other federal entities and the private sector are doing in threat detection technology? Do you have personnel dedicated to seeking out such technologies to inform agency work and to avoid potential duplication of efforts? Finally, how do you ensure that the threat detection technologies developed through federal research funding will be both economical and usable?

Response: The Department of Homeland Security (DHS) Domestic Nuclear Detection Office (DNDO) engages with the private sector, national laboratories, and the academic community to advance knowledge for nuclear and radiological threat detection and related sciences with emphasis on fundamental research to solve long-term, high-risk challenges or dramatically improve the performance of radiological and nuclear detection systems and enabling technologies.

To ensure efficient and effective use of research and development (R&D) funding, there are mechanisms in place for coordination across federal entities and their respective programs to ensure awareness of activities and prevent unnecessary duplication of efforts. R&D specifically focused on nuclear detection is coordinated to ensure that work addresses the needs identified by the global nuclear detection architecture (GNDA). Further, DNDO coordinates with the National Institute of Standards and Technology (NIST) and private sector Standards Development Organizations (SDOs) to develop and promote the use of voluntary consensus based radiation detection standards to ensure a robust, fair and informed marketplace for American manufacturers and researchers working on the next generation of detection technologies.

For basic and applied research, DNDO coordinated a multi-agency memorandum of understanding between DHS, the Office of the Director of National Intelligence, Department of Energy (DOE), and Department of Defense (DoD) to integrate R&D programs. The signatories participate in each others' program reviews and proposal evaluations, and provide full and open access to programs and their findings.

DOE, DoD, and DNDO hold annual conferences for basic and applied research efforts that aid in minimizing duplication and facilitating collaboration to integrate research efforts to have greater impact. DNDO's extensive Test and Evaluation (T&E) efforts are supported by NIST measurements, technical guidance and assistance during testing, standardized radioactive sources, and data analysis. DNDO maintains a database of interagency testing results. Agencies across the government are now able to more easily

Question#:	1
Topic:	federal entities
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Ralph M. Hall
Committee:	SCIENCE (HOUSE)

assess whether current technology or commercial systems are available to meet their needs without initiating unnecessary or duplicative R&D and test and evaluation efforts.

DNDO also actively participates in interagency processes to develop interagency goals for R&D, in particular, the Nuclear Defense R&D (NDRD) Roadmap led by the Office of Science and Technology Policy (OSTP). The NDRD Roadmap is a joint assessment of gaps and priorities for the R&D needs of the GNDA and technical nuclear forensics, and guides U.S. Government R&D investment.

Finally, DNDO regularly issues Requests for Information (RFIs) to the private sector in order to maintain awareness of the current developments and marketplace for radiological and nuclear detection technologies. RFIs are posted to Fedbizops.gov (www.fbo.gov) and are a regular part of DNDO's transparent and competitive solicitation process. Industry responses provide information about commercial systems in a range of different applications.

DNDO works closely with end-users to identify, develop, and acquire appropriate solutions that meet operational needs and requirements.

Question#:	2
Topic:	difficulties
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Dan Benishek
Committee:	SCIENCE (HOUSE)

Question: Your testimony mentions the inherent technical difficulties in developing nuclear detection technologies for homeland security applications (including limitations related to speed, distance, shielding, and source strength). How is each of your agencies working to improve the ability of technologies to detect threats in challenging environments?

Response: DNDO's transformational R&D program seeks to identify, explore, develop, and demonstrate scientific and technological approaches that address gaps in the global nuclear detection architecture (GNDA), dramatically improve the performance of nuclear detection components and systems, and/or significantly reduce the operational burden of radiological/nuclear detection.

DNDO R&D efforts seek to develop cost-effective, mobile, and agile systems that can be widely deployed, and include interesting and novel ways to network detectors to enhance wide-area search capabilities. DNDO continues to work on technologies to detect shielded special nuclear material.

For example, DNDO's Advanced Radiation Monitoring Device (ARMD) project focuses on enhancing our ability to distinguish benign radiological and nuclear materials, from those that potentially pose a threat. Through this project, we have identified two materials that have greater efficiency and energy resolution, allowing development of smaller, more capable detection systems using strontium iodide or cesium lithium yttrium chloride crystals. Coordinated interagency work between DNDO, DoD's Defense Threat Reduction Agency, and DOE have pushed the materials to maturity where they are now commercially available for use in detector systems.

Question#:	3
Topic:	helium-3
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Ben Lujan
Committee:	SCIENCE (HOUSE)

Question: The shortage of helium-3 affects our ability to detect nuclear threats. What is the state of development of helium-3 alternative technologies and when should we expect to see them deployed?

Response: DNDO has been leading U.S. Government efforts to pursue alternative technologies to helium-3 (^{3}He) based neutron detectors. In February 2011, DNDO released a Request for Proposals (RFP) for the Neutron Detector Replacement Program to solicit near-term commercial neutron detection technologies for radiation portal monitor (RPM) applications. DNDO then sponsored a test campaign from June through August 2011, and identified two commercially available alternative technologies that have sufficient capability for neutron detection in an RPM, which meets or exceeds current ^{3}He neutron detection performance. The identification of these commercial technologies as viable replacement technologies for ^{3}He neutron detectors will allow the Department to leverage market forces to find the best value for any future procurement.

Additionally, DNDO performed a separate evaluation of a technology that was based on Boron-10 lined tubes. The DNDO test effort included an initial assessment of the technology against performance specifications and a field validation effort with the alternative neutron detection technology integrated into an RPM system. Based upon the test results, the RPM system with the boron-10-lined tubes (alternative neutron detector) was also demonstrated to be an adequate alternative to the ^{3}He neutron detection modules currently in use for cargo scanning configurations.

In April 2012, DNDO conducted a rigorous, interagency test of backpack, handheld, vehicle-mounted and portable neutron detection. This test campaign investigated potential alternatives to ^{3}He based neutron detectors for the aforementioned classes of systems. During this test, 39 different neutron detection technologies were evaluated, and the test data was provided back to the participating vendors to accelerate and focus their ability to address the DHS requirements.

DNDO plans to conduct additional testing in 2013 and anticipates that the commercial sector should be ready to provide alternative technologies for all the typical radiation detection systems (handheld, backpack, and mobile systems) deployed.

Question#:	4
Topic:	helium-3 replacement
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Ben Lujan
Committee:	SCIENCE (HOUSE)

Question: Which government agencies played substantial roles in developing the Helium-3 replacement technologies? What research institutions provided the basic research? Is there adequate work taking place in basic research in detection materials?

Response: DNDO worked closely with DOE and DoD to address alternative neutron detection technologies that could replace ^{3}He.

Since 2009, DNDO has been a major contributor to addressing the ^{3}He shortage within the interagency. DNDO was a founding member of the interagency ^{3}He Integrated Project Team (IPT) and supported the effort by providing the ^{3}He IPT Chairman and Technology Working Group lead until October 2011. An Interagency Policy Committee was formed in 2009 and provided the Government with guidelines for ^{3}He distribution and allocation.

DNDO worked with national laboratories, universities, and industry to perform basic research through our Exploratory Research project for Neutron Detection including Helium-3 Alternatives. This project explores near-term and longer-term alternatives to ^{3}He neutron detectors currently used in various radiation portal monitor (RPM) applications, as well as backpack, handheld, and personal radiation detection instruments. Particular focus was initially on portal applications since this requires the most ^{3}He, but increasing attention is being given to applications which are the next largest users of ^{3}He – backpacks and handhelds. This project investigates a range of materials, technologies, and sensor systems, many of which are based on either boron-10 or lithium-6 as neutron capture agents. This project also explores novel techniques for fast neutron detection.

Question#:	5
Topic:	Nuclear forensics
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Ben Lujan
Committee:	SCIENCE (HOUSE)

Question: Nuclear forensics plays a key role in threat detection. Yet a National Research Council report from a couple of years ago found that the Nation's nuclear forensics capabilities are fragile, under resourced and in some respects deteriorating. What is your opinion of the state of the government capability in this area? Is there sufficient support for research, development, operations and infrastructure?

Response: The 2010 National Research Council report "Nuclear Forensics: A Capability at Risk" highlighted areas where the U.S. Government needed to focus on leadership, planning, and funding. The report also emphasized the fragility of technical nuclear forensics (TNF) capabilities and the need for additional resources, while noting that such capabilities "can contribute substantially to deterring, limiting and responding to nuclear terrorism."

Comprehensive assessments of needs, shortfalls, and priorities for TNF have taken place and continue across the six executive branch departments involved in nuclear forensics activities, as well as the National Security Staff and Congress. The report's recommendations have been embraced by all partner agencies. Notable improvements have been taking place across the TNF spectrum from creating the first-ever TNF Requirements Center in DNDO, to more rigorous full-scale exercises, to advanced technology demonstrations.

Because of this increased focus and attention on TNF at the highest levels of government, the support for TNF-related programs has grown and solidified. Since the establishment of NTNFC in DNDO in FY 2007, our TNF budget has increased by more than 70% and stabilized at this level. Within the annual budget for NTNFC, approximately 50% is devoted to near-term R&D, while the other 50% is allocated across operational readiness, expertise development, and other priorities. Additionally, DNDO's Transformational Research and Development directorate invests in promising long-term R&D projects. This level of expenditure enables DNDO to continue pursuing the recommendations of the National Research Council, as well as the investment priorities of the President's National Strategic Five-Year Plan.

Question#:	6
Topic:	test
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Ben Lujan
Committee:	SCIENCE (HOUSE)

Question: It is extremely important to test threat detection technology in a realistic manner. Does the Nation have realistic test and evaluation capabilities for the threats that range from nuclear and explosive to chemical and biological? For example, do we have adequate capability to test radiation-detection gear with real threat materials such as special nuclear materials?

Response: As you note, it is extremely important to conduct both technical performance testing and operational assessments of radiological and nuclear (rad/nuc) detection technologies using realistic threat signatures and operationally relevant concepts of operation (CONOPS), in order to understand the performance and limitations of these systems. To address the technical performance of these technologies, DNDO and the National Laboratory partners utilize the performance criteria and testing methods outlined in the ten DHS adopted ANSI/IEEE radiation and nuclear detection equipment standards. To address threat detection for rad/nuc threats, DNDO has worked with our National Laboratory partners to research, develop, manufacture, and deploy unique radiation signature training devices for use in our performance testing and operational assessment programs. Radiation signature training devices allow DNDO to evaluate system performance against realistic signatures of actual highly enriched uranium and weapons-grade plutonium.

DNDO's Red Team also uses radiation signature training devices to present adversary scenarios to various Federal, state, and local operational elements. The radiation signature training devices present operators with signatures that are not normally seen in daily operations and provide a unique opportunity to detect threat material and then exercise the adjudication process from the point of detection up through various levels of analysis and response. To date, DNDO has conducted over 60 overt and covert operational assessments with our Federal, state, and local operational partners.

DNDO also uses radiation signature training devices, as well as other special nuclear material and radiological sources, to conduct rigorous performance testing of rad/nuc detection systems being developed and deployed. DNDO maintains highly specialized and secure testing facilities, such as the Rad/Nuc Countermeasures Test and Evaluation Complex at the Nevada National Security Site, to conduct such test campaigns using realistic source configurations and CONOPS. Since 2005, DNDO has conducted over 70 test and evaluation campaigns covering all classes of detection systems; including

Question#:	6
Topic:	test
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Ben Lujan
Committee:	SCIENCE (HOUSE)

personal radiation detectors, handheld radio-isotope identification devices, backpacks, vehicular or aerial mounted mobile systems, and radiation portal monitors.

DNDO does not develop or test chemical, biological, and explosive detectors, and questions on those should be directed to the relevant Federal agencies.

Question#:	7
Topic:	unique
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Randy Neugebauer
Committee:	SCIENCE (HOUSE)

Question: What is unique about the development of technologies designed to detect intentional threats versus accidental threats or natural disasters?

Response: Because nuclear accidents or natural disasters (e.g., Fukushima) typically release large amounts of radiation, detector systems used during an accident or disaster only need to measure enough radiation to warn an individual of health dangers and to help facilitate clean up. Thus, the main function of a radiation detector used in response to an accidental threat or natural disaster would be to determine the ionization, or dose rate, being absorbed by people from a known radiation source, in order to facilitate protection of the public.

In contrast, when using a radiation detector to detect intentional threats, the operator seeks to search areas, people, or conveyances to find and identify a threat material. Additionally, the radiation signature from a nuclear threat is potentially small, especially during storage or transit when a terrorist may try to conceal the radiation signature to prevent detection. As such, detectors used to prevent a threat need to be significantly more sensitive than detectors used to respond to an event.

Question#:	8
Topic:	commercial first
Hearing:	Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Primary:	The Honorable Randy Neugebauer
Committee:	SCIENCE (HOUSE)

Question: The Domestic Nuclear Detection Office (DNDO) has recently shifted to a "commercial first" approach for technology development, which is designed to take advantage of industry's innate flexibility and ability to rapidly improve technologies. Has this approach been successful thus far? What challenges has DNDO faced?

Response: The "Commercial First" approach is based on the principle that all DNDO programs will engage the private sector for solutions to address the gaps identified in the GNDA prior to moving into a government sponsored and managed development effort. There are several "Commercial First" pathways that a program can follow depending on the defined gap, the technical maturity, and commercial availability of potential materiel solutions that may be able to address that gap. These pathways include:

- Commercial off the shelf (COTS)
- Customized COTS
- Commercialization (e.g. Commercial Development)
- Government Sponsored Development

DNDO initiated the "Commercial First" approach with the Human Portable Tripwire (HPT) program in November 2011. The HPT program is an effort to identify and develop more capable personal radiation detection devices for use by Federal, state, and local law enforcement officials as part of their standard equipment.

At the November 2011 Industry Day for the HPT program, DNDO provided information to private sector participants about the requirements for commercially-developed technology solutions, so vendors can tailor their products. Other DHS Components, including U.S. Customs and Border Protection, U.S. Coast Guard, and the Transportation Security Administration, as well as state and local organizations, also discussed their operational needs for current and future radiation detection systems.

Responses by Dr. Anthony Peurrung

House Committee on Science, Space, and Technology Questions for the Record
Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Thursday, July 19, 2012
Dr. Tony Peurrung, Pacific Northwest National Laboratory

Question from the Honorable Ralph Hall (R-TX)

1. How do your agencies stay up to speed on what other federal entities and the private sector are doing in threat detection technology? Do you have personnel dedicated to seeking out such technologies to inform agency work and to avoid potential duplication of efforts? Finally, how do you ensure that the threat detection technologies developed through federal research funding will be both economical and usable?

   To maintain awareness of research and development (R&D) efforts within the National Security enterprise, the Pacific Northwest National Laboratory (PNNL) employs a number of approaches to provide us with a reasonable view of the R&D landscape and help us identify technical gaps and emerging issues that require new solutions. The unusually high degree of security, related sensitivity, "need-to-know," and classified nature of the work adds a significant barrier to maintaining awareness of ongoing work across the United States Government.

   One of these approaches, our attendance at national meetings, conferences and symposia, including classified reviews, is an important element to our overall effort to maintain awareness. At these meetings we contribute to the information sharing about our own research and successes stories and learn about work being funded elsewhere. These meetings serve an important function in connecting the research community, building peer-to-peer relationships and partnerships, obtaining peer review, and sharing ideas and knowledge about particular technical problems.

   Another method relies heavily upon regular engagement with our clients to understand their most pressing science and technology (S&T) needs, and to identify capabilities within PNNL that can help to develop solutions. Through this dialogue we learn about work our clients are already funding and (to the extent they are aware) of complementary research outside their organization. Many of our clients participate in some level of interagency coordination across the mission space and they possess a level of knowledge about R&D efforts across the government.

   PNNL also frequently hosts visits by senior government officials including R&D directors, program managers, and chief scientists from organizations that fund R&D in the technical areas we serve. These visitors represent a cross cut of agencies in the United States Government, and in particular the National Security enterprise. We generally provide briefings on our research efforts that are relevant to their particular areas of interest, and we learn from them about related work elsewhere. Because of our diverse client base we are able to gain insights that might not have been obvious to a casual observer.

   Finally, the last major element of our approach to maintaining awareness is through the information-sharing, internal peer review, and science and technology coordination functions that are inherent within the PNNL capability development processes. For example, the allocation of discretionary resources for building new capability and testing novel concepts involves several layers of technical review and competitive assessment. When PNNL makes a multi-million dollar capability development investment in a particular technical area, it often creates a large-scale internally funded project. External advisory groups are established for each of these major projects and one of their tasks is to assess the uniqueness and value of the R&D efforts. We rely on these advisors' periodic review of the progress to help us identify other relevant research. In the end, we help ensure that the research funded is both economically feasible and usable in the real-world.

Question from the Honorable Eddie Bernice Johnson (D-TX)

1. In fiscal year 2012, the research and development activities of the Department of Homeland Security's Science and Technology (DHS S&T) were cut by more than 38 percent compared to fiscal year 2010, resulting in DHS S&T having to stop a number of ongoing projects, significantly reduce others and forgo any new research and development initiatives, including critical research efforts in biological defense, cybersecurity, border security, and first responder technology. In your written testimony, you note that approximately half of PNNL's business is centered on national security missions. Can you tell us how PNNL has been impacted by recent congressional budget cuts at DHS S&T?

   The budget cuts that DHS S&T took in fiscal year (FY) 2011 and 2012 had significant impacts on many of the National Laboratories. Since I am most familiar with PNNL, I will focus on the impacts to PNNL, but each of the National Laboratories could provide similar challenges due to the recent budget cuts. At PNNL, a number of important projects that PNNL managed for DHS S&T were either eliminated altogether or significantly cut back in several domain areas, including explosives detection, infrastructure protection, and information analytics. Not only did the cuts have impacts at PNNL, but also for our many university partners across the Nation. Examples of the research projects that were affected by the budget cuts are described below.

   - **Wide-Area Surveillance Project.** PNNL partnered with the Massachusetts Institute of Technology Lincoln Laboratory to develop a prototype system for persistent surveillance of wide areas. The prototype was piloted at Boston's Logan Airport in FY 2010 and FY 2011 with enthusiastic support from transportation agencies, state emergency response agencies, and industry with the hope that it could be used in other large venues for persistence surveillance.

   - **Standoff Detection Integrated Demonstration Project.** This project sought to accelerate the development and deployment of explosives countermeasures using standoff technologies to allow for the non-intrusive, non-checkpoint screening of large numbers of people at sporting arenas, malls, transportation hubs, and the battlefield. PNNL's partners in this project included Northeastern University and its DHS Center of Excellence partners.

   - **Resilient Tunnel Project.** This project used advanced materials to develop and deploy inflatable plugs that prevent tunnels from flooding during natural or intentional disasters. The full-scale prototype was to be tested in FY 2012 but had to be delayed. The project has received high interest from transit authorities as a way to save the lives of first responders and the public in New York and elsewhere. PNNL partnered with West Virginia University and industrial partner ILC Dover for this project.

- **Precision Information Environments.** This project allows the many emergency response agencies to engage with each other and leverage their collective expertise and experience in a "reality-based" environment to support actions, assessments, and decision making. Stakeholders across the country, particularly in the Northwest, have weighed in on the development of these advanced information technologies, and prototypes are in development. Lack of FY 2012 funding had to stop this work.

The researchers and staff members assigned to these and other projects that were eliminated or postponed had to transition to other projects across the Laboratory. We may lose the project expertise these individuals hold because they may not return to the project if DHS S&T chooses to resume funding. As I stated in my written testimony for the Committee, although extremely valuable, science programs targeted at pressing national security threats are fragile. They can be harmed, not only by the inevitable fluctuations in funding support, but also by rapid shifts in the leading threat of the day or by excessively short-term objectives. I continue to recommend that strategic stewardship of our threat detection research capabilities and the science that underlies them remain a high federal priority.

Question from the Honorable Dan Benishek (R-MI)

1. Dr. Gowadia's testimony mentions the inherent technical difficulties in developing nuclear detection technologies for homeland security applications (including limitations related to speed, distance, shielding, and source strength). How is your laboratory working to improve the ability of technologies to detect threats in challenging environments?

   Developing functional technology for field environments is a challenging pursuit that requires knowledge of the underlying science behind nuclear detection, the possibilities offered by engineered sensor solutions, and the constraints imposed by operating technology in the field. PNNL is developing a suite of next-generation technology solutions by leveraging scientific knowledge and capability across detection systems, mathematical analysis, decision science, and signature discovery.

   High-fidelity Sensor Systems

   PNNL is pushing the limits of exploiting physical signatures from nuclear material for threat detection. This requires building specialized technology that does not exist in the commercial sector today. For example, one project funded by the National Nuclear Security Administration (NNSA) and demonstrated in a joint program by the Technical Support Working Group and the Defense Threat Reduction Agency developed a compact array of high-resolution semiconductor detectors for detection of gamma rays. The high resolution of these sensors enables characterization of the nuclear material that in turn leads to actionable identification when encountering highly enriched uranium, plutonium, or other threats. Radioactive materials—benign sources—such as medical and industrial isotopes and naturally occurring radiation are routinely found in items of commerce and often confuse existing systems. This system, termed MARS, is less susceptible to falsely identifying nuisance sources as threatening material. PNNL's sensor system also increased the distance at which potential threat sources could be detected and characterized. It addressed operational challenges and was successfully demonstrated on an unmanned surface vessel at the Federal Law Enforcement Testing Facility (FLETC) in

Charleston, South Carolina and in Southeast Asia. The system was recently part of a successful performance evaluation (funded by NNSA) aboard a Bell 412 helicopter.

Unattended Sensors and Compact Systems

Two key challenges to sensor development are the need for smaller, less invasive technology and the engineering of systems that can operate in an unattended mode, thus reducing the demands on operators. PNNL is developing the next generation of sensors systems that in some cases incorporate new detection materials. The goal of this effort is to develop technology that enables automated threat detection that can alert law enforcement to the presence of nuclear material while simultaneously reducing nuisance alarms caused by benign sources of radioactivity. Currently under development through sponsorship by NNSA, PNNL's system incorporates cutting-edge radiation detection materials developed commercially and allows the simultaneous detection of gamma-ray and neutron emissions from nuclear material using the same radiation detector.

Advanced Algorithms

There is a potential for improvement in threat detection technology in the realm of developing algorithms to improve a detector's interpretation of sensor data. PNNL brings a cross-disciplinary expertise linking physicists, engineers, and mathematicians to devise novel concepts that exploit data from existing systems. One challenge is to discriminate the array of benign sources that exist in the stream of commerce from nuclear materials that are of proliferation concern. Sometimes these algorithms must be deployed in low-power unattended systems that demand computational simplicity. In other cases, sophisticated algorithms based on the latest statistical analysis tools can be adapted to nuclear detection technology. Regardless of the algorithm, the goal of PNNL's development is to exploit data collected from sensors deployed in the field.

Signature Discovery

Nature imposes fundamental limits to current technology performance. Nuclear material emissions can be obscured from detection technology. Therefore, transformational changes in detection performance require discovery and exploitation of new signatures or composite analysis of existing signatures. PNNL is making a major internal investment into the development of signature discovery methods and tools to exploit signatures in complex data streams. A key ingredient of this approach is to fuse information streams that allow targeting of potential threats with the development and deployment of physical sensors and collection of samples for laboratory analysis. An example is the development of tools to analyze social media, searching for indicators of potential illicit nuclear material trafficking networks, which can then direct the deployment of physical sensors to targeted geographic regions. In this model, detection capability can surge to the highest-risk locations, creating an efficient method of resource allocation. One immense challenge to this aspiration is the prerequisite of real-time integration of multiple data streams. Developing tools that distribute analytical capability to various information collection points is an essential technical challenge that must be overcome.

Training

Training is essential to achieving the risk reduction return on investment from the radiation detection technologies that have been deployed around the globe. This is especially true of foreign partners who operate these special technologies in challenging or even hostile environments. In response, PNNL developed a world-renown academy-level training program that instructs both United State Customs and Border Protection officers and foreign partner stakeholders to better understand the threats associated with weapons of mass destruction and how to effectively use commercially available technology to deter, detect, identify, and interdict the illicit movement of proliferation concern materials. The PNNL-developed training curriculum prepares front-line officers on the use of the radiation detection equipment, recognition of common smuggling tactics and techniques, operational procedures, maintenance practices, and appropriate response protocols. An integral part of this training is to familiarize operators with the inherent limitations of the radiation detection systems and how to properly interpret data generated from the systems to ensure threat and other suspicious materials receive proper attention before entering the United States.

Questions from the Honorable Ben Luján (D-NM)

1. The shortage of helium-3 affects our ability to detect nuclear threats. What is the state of development of helium-3 alternatives technologies, and when should we expect to see them deployed?

   There are a number of technologies that are acceptable replacements for the majority of the nuclear threat detection programs. The exception may be compact human portable detectors where helium-3 may be required, given the operational constraints of such systems. There are a number of commercial alternatives to helium-3 that vendors are marketing and incorporating into their product lines now. What is needed is a thorough evaluation by the programs deploying such sensors to determine their suitability, both from a detection efficacy perspective, and suitability to operational environments.

2. Which government agencies played substantial roles in developing the helium-3 replacement technologies? What research institutions provided the basic research? Is there adequate work taking place in basic research in detection materials?

   PNNL is aware of three major detector material research programs in the United States Government that focus on nuclear threat detection research and development. They are the Department of Energy's (DOE) NNSA Office of Nonproliferation and Verification Research and Development Advanced Materials Program, the Department of Homeland Security's Domestic Nuclear Detection Office's (DNDO) Transformational and Applied Research Directorate, and the Department of Defense's Defense Threat Reduction Agency's Nuclear Threat Detection portfolio. While PNNL is not privy to the full extent of these programs' investments, it is aware that these three portfolios represent the vast majority of investment in new detector materials for nuclear threat detection.

   A number of academic institutions work in the area of advanced detector material R&D. We are not privy to the extent of which institution is funded to pursue this area of R&D.

   PNNL is not in a position to access the breadth and extent of the federal government allocation of funds to this issue. It is, however, evident in the scientific literature and at scientific conferences that this issue is getting broad attention across the research and development community.

3. It is extremely important to test threat detection technologies in a realistic manner. Does the Nation have realistic test and evaluation capabilities for the threats that range from nuclear and explosive to chemical and biological? For example, do we have adequate capability to test radiation-detection gear with real threat materials such as special nuclear material?

   The Nation possesses a number of facilities that allow for the use of realistic tests associated with a variety of different threats. For instance, PNNL possesses broad capabilities to test detector systems with special nuclear material (SNM). These capabilities allow testing of systems from early-stage laboratory prototypes up to fully integrated commercial systems. The facilities can be configured to represent real-world environments across the land, rail, sea, and air venues, and offer controlled environments where special nuclear material can be introduced. PNNL has broad experience in test and evaluation in the field.

   In addition to PNNL capabilities there are a number of other DOE national laboratories that possess varying levels of test and evaluation facilities with access to SNM. The Radiological/Nuclear Countermeasures Test and Evaluation Complex (RNCTEC), operated on the Nevada Test Site by DNDO for test and evaluation, is a dedicated facility that has access to a diverse set SNM unique to that facility. Collectively these capabilities give the Nation the broad ability to test equipment against real threats in simulated operational environments.

   The Nation has some limited capabilities for the realistic test and evaluation of chemical and biological threats. While multiple laboratories can handle chemical and biological agents, it is much more challenging to also generate realistic environmental conditions for testing technologies for chemical and biological detection, protection, and decontamination. A robust test and evaluation process would require testing at more than one location. Testing laboratories must be secure and have expertise in the threats as well as experimental design and data analysis. Rigorous quality control is essential.

Question from the Honorable Randy Neugebauer (R-TX)

1. What is unique about the development of technologies designed to detect intentional threats versus accidental threats or natural disasters?

   The biological threat is often difficult to distinguish between intentional versus accidental or naturally occurring. In order to protect our communities and natural infrastructure from biological threats the ability to rapidly detect and respond to an infectious outbreak and determine its origin is imperative. The response to any given outbreak is dependent upon whether the originating agent was released intentionally or is simply the result of a common natural cycle. Currently, the ability to distinguish between a natural outbreak and an intentional release is dependent upon a range of highly specific bioanalytical techniques. These techniques are focused on two complementary areas: threat agent identification and threat agent characterization.

   Except in rare cases, the majority of biothreat agents are found in the natural environment throughout the world. This fact is the primary reason that makes distinguishing a natural event from an intentional release a significant scientific challenge. Natural outbreaks usually occur following an environmental disturbance such as a hurricane, flood, or dust storm in which a typically dormant biological agent can come into contact with a plant, animal, or human population.

Historically, deployed detection systems have focused exclusively on threat identification using genetic methods, and remain largely unmatched by other approaches. Unfortunately, the genetic code of a biological threat agent does not always contain information required to determine whether an outbreak was the result of an intentional release. This level of discrimination requires additional techniques capable of distinguishing whether an organism was cultivated in a laboratory setting or in the environment. These approaches draw upon a range of scientific disciplines and focus on topics related to fundamental biology and trace chemical analysis. These non-genetic signatures include biochemical profiles, chemical element concentrations, and the presence or absence of chemicals commonly used to stabilize biological threat agents for an intentional release. Other non-genetic signatures that may be useful in a forensic capacity include trace impurities that remain during the growth and preparation of a biological agent intended for release.

In addition to the technological approaches and scientific teams capable of distinguishing between a natural outbreak and an intentional release, there is still strong need for effective reporting, data sharing, and interactions among numerous agencies and countries to effectively detect a disease outbreak, let alone the source or intent of the outbreak. The current state-of-the-art rapid biodetection platforms require up-front selection of the pathogens of most concern to be screened and may not detect genetically modified or purposefully altered pathogens meant to do additional harm and/or avoid common detection.

DHS S&T is funding PNNL to develop tools to identify signatures of man-made culturing of microorganisms and to detect additives that could be signatures for an intentional release of a bioagent. In addition, PNNL is evaluating man-portable, commercially available detection systems to rapidly detect the identity of the threat agent.

Finally, there is also a strong technology development emphasis across the research community to compile many different open sources of information to provide early alert of a potential new bioagent outbreak—whether intentional, accidental, or natural. These global biosurveillance efforts focus on integrating textual data, social network feeds of illness reporting, monitoring of pharmacy purchases, school and workplace attendance, and other abnormal behavioral changes to a typically healthy community. It is becoming more apparent that monitoring animal populations and environmental reservoirs may also help alert to a potential biohazard threat more rapidly than clinical reporting alone.

Responses by Dr. Thomas Peterson

Keeping America Secure: The Science Supporting the Development of Threat Detection Technologies
Thursday, July 19, 2012
Dr. Thomas Peterson

1. Questions from the Honorable Ralph Hall

(a) How do your agencies stay up to speed on what other federal entities and the private sector are doing in threat detection technology?

ANSWER:

The National Science Foundation (NSF) has multiple partnerships with other agencies, some of which are described in Dr. Peterson's testimony. Among these partnerships are those with the Department of Homeland Security (DHS), Defense Threat Reduction Agency (DTRA), and National Geospacial Intelligence Agency (NGA). See, for example, the following links:

http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503427

http://www.nsf.gov/news/news_summ.jsp?cntn_id=108398

http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503223

Through NSF's "Industry University Cooperative Research Center (I/UCRC)" program, NSF develops liaisons with private industry who are active in specific areas, including those industry segments addressing threat detection technologies. Federal agencies comprise 15% of all I/UCRC membership support, and large and small business comprises over 75%. Industry and government members work in partnership with center universities to assure the center's research portfolio addresses unmet research needs and complements existing efforts in the private and government sectors. Federal members of I/UCRCs network across government in their sectors. For example the Member Advisory Board Chair of the I/UCRC for Identification Technology Research (referenced in Dr. Peterson's testimony) is a DHS Program Director. He is also the co-chair of the National Science & Technology Council (NTSC) Subcommittee on Biometrics and Identity Management composed of representatives from all federal agencies using biometric technology.

Additionally, a number of NSF's standard research grants involve private industry partners (see Dr. Peterson's testimony for examples).

(b) Do you have personnel dedicated to seeking out such technologies to inform agency work and to avoid potential duplication of efforts?

ANSWER:

NSF does not have personnel dedicated solely to such activity, but instead such activity is part of the portfolios of several program officers in various directorates, including Engineering (ENG), Mathematical

& Physical Sciences (MPS), Computer & Information Science & Engineering (CISE), and Social, Behavioral & Economic Sciences (SBE).

NSF participates in a number of Office of Science and Technology Policy (OSTP) groups and other interagency coordination focused on addressing threat issues.

(c) Finally, how do you ensure that threat detection technologies developed through federal research funding will be both economical and usable?

ANSWER:

Because NSF funds basic research, it relies on its partnerships with mission agencies for the evaluation of economics and usability. For example, research grants made by NSF under the Domestic Nuclear Detection Office (DNDO)/DHS-NSF partnership are transferred to DNDO after the initial year, for evaluation of progress and promise, as well as supervision and further funding (if warranted).

Possibilities for major breakthroughs in usability, relevance and "bang for the buck" are high on the list of what we would ask panelists to look for in evaluating research proposals, and in guidance we give at grantees' conferences. We have had some discussion about whether focused workshops would be useful in better illuminating the strategic landscape of high-risk possibilities for larger breakthroughs in this area.

2. Question from the Honorable Dan Benishek

Dr. Gowadia's testimony mentions the inherent technical difficulties in developing nuclear detection technologies security applications (including limitations related to speed, distance, shielding, and source strength). How is the National Science Foundation working to improve the ability to detect threats in challenging environments?

ANSWER.

The inherent technical difficulties are very serious and sobering. NSF's primary means of trying to address those difficulties have been:

- use of scientific panel discussion (see questions 1) in review of ARI proposals,
- thoughtful discussions with partners at DNDO after reading some of their written material, and
- modest participation in ARI grantees' conferences.

Some of the technical difficulties (such as the difficulty of detecting shielded highly enriched uranium at a distance) are deeply rooted in our practical understanding of how the physics works. These are hard problems and the joint NSF-DNDO Academic Research Initiative (ARI) effort has several ongoing fundamental research projects that are addressing them.

NSF has partnered with DNDO/DHS and other agencies to support fundamental research at universities, sometimes in collaboration with private industry, on this topic (see links above).

3. Question from the Honorable Ben Lujan

It is extremely important to test threat detection technology in a realistic manner. Does the Nation have realistic test and evaluation capabilities for the threats that range from nuclear and explosive to chemical and biological? For example, do we have adequate capability to test radiation-detection gear with real threat materials such as special nuclear materials?

ANSWER.

NSF does not have these capabilities, but is partnered with agencies, such as DHS and Department of Defense (DOD), that do.

DTRA carries out this type of work at the Technical Evaluation Assessment Monitor Site (TEAMS) in Albuquerque, and with partners at the Nevada National Security Site and Idaho National Labs.

Operations-level facilities for testing nuclear detection equipment are a specialty of the National Labs and of other agencies, not NSF.

Initial laboratory testing, unique to each project, is a standard part of research projects in this area. Adequacy of empirical testing in any given project is part of what review panels normally discuss and evaluate in deciding what to recommend for funding; in some cases, the research includes collaborations with national labs for subsequent testing.

4. Question from the Honorable Randy Neugebauer

What is unique about the development of technologies designed to detect intentional threats versus accidental threats or natural disasters?

ANSWER.

Intentional threats include IEDs, chemical explosives laced with radioactive materials ("dirty bombs"), "small" nuclear bombs, poison gas, biological weapons (such as weaponized anthrax), etc. Accidental threats and natural disasters include chemical and oil spills, gas leaks, nuclear plant failures (sometimes caused by natural disasters), burst water mains, floods, earthquakes, tsunamis, hurricanes, tornadoes, wildfires, etc. Intentional threats are covert and hidden by human design, while accidental threats and natural disasters are not. As a rule (there are exceptions), the technologies required to detect intentional threats (e.g., IEDs) are of a different character than those for detecting natural disasters (tornadoes) or accidental threats (e.g. oil spills).

The difference between methods and systems to address natural threats and methods to address malicious threats is quite fundamental, even when we design systems like power grids to cope with both. The main difference is that when we cope with malicious threats, our models and analysis must account for the presence of intelligent adversaries, who try to be extremely creative about focusing on the weakest link of any system we may devise. For example, if we build a system which is provably stable or safe under certain assumptions, an intelligent adversary will typically focus on things which go outside of our normal assumptions.

Natural hazards of tornadoes, hurricanes and earthquakes are recorded by federal agencies such as US Geological Survey(USGS) and National Oceanic and Atmospheric Administration(NOAA). The data base of these hazards goes back to 60 to 100+ years.

Tornadoes are recorded by NWS regional offices when they occur in their regions. Based on the damage, length and path (the area affected by tornado) are recorded. And based on the level of damage, intensity of a tornado is recorded as EF – Scale; the scale is from EF0 to EF5. EF stands for Enhanced Fujita scale. Each scale is assigned wind speed range. NWS/NOAA started keeping records since around 1970 when Dr. Ted Fujita at University of Chicago developed Fujita Scale. Storm Prediction Center, SPC/NOAA reviewed news papers and other sources to assign Fujita scale to recorded tornadoes since 1950. NWS changed F – scale to Enhanced Fujita, EF – Scale starting February 2007.

Hurricanes are recorded by National Hurricane Center, NHC/NOAA by satellite images in recent years. The parameters recorded for hurricanes are barometric pressure in the eye, diameter of eye, maximum wind speed, diameter of damaging wind speed, speed of the storm movement, storm track etc. NHC/NOAA has gone back in the archive and has assembled database since late 1800s. For public announcement NHC uses Saffir-Simpson Scale for hurricanes from Category 1 through 5. Each Category has a range of wind speed.

Earthquakes (the following is exerpted from: http://pubs.usgs.gov/fs/2011/3021/pdf/fs2011-3021.pdf):

"The U.S. Geological Survey's National Earthquake Information Center reports on more than 30,000 earthquakes a year worldwide, automatically detecting, locating and characterizing events, providing alerts, maps of strong ground shaking, and impact estimates of potential fatalities and losses. These rapid earthquake information products, which enable the prompt mobilization of emergency resources by all levels of government and humanitarian organizations, depend on the high quality seismic stations that make up the Global Seismographic Network...Nearly all GSN stations transmit data in near real-time"..."GSN data enabled the USGS National Earthquake Information Center to provide within 30 minutes a project of the impact of the devastating 2010 Haiti earthquake"..."In addition, more than 50 stations of the GSN are part of the International Monitoring System of the Comprehensive Test Ban Treaty Organization (CTBTO) and contribute to nuclear test monitoring and treaty verification." (From Gee, L.S., and Leith, W.S., 2011, The Global Seismographic Network: U.S. Geological Survey Fact Sheet 2011–3021, 2 p.)

"The Global Seismographic Network (GSN) is a permanent, digital network of more than 150 modern stations in over 80 countries, from the South Pole to Siberia and from the Pacific basin to the southern tip of Africa. At the core of the GSN, are the very broadband, high-dynamic range seismometers that measure the vibrations of the Earth. These instruments are extremely sensitive over a wide range of frequencies and are capable of detecting the response of the Earth to the motions of the Sun and the Moon with periods of thousands of seconds, as well as the strong shaking near large earthquakes with periods less than a tenth of a second, with high fidelity. In many cases, these seismometers are combined with other sensors, such as microbarographs, anemometers, magnetometers, and Global Positioning System receivers, to form geophysical observatories. Advanced systems for data acquisition and communications transmit continuous digital data from the stations to collection points in the U.S. The GSN was formed in 1986 as a partnership involving the U.S. Geological Survey (USGS), the National Science Foundation (NSF), and the Incorporated Research Institutions for Seismology (IRIS, a university consortium) and serves as a multi-use scientific facility and societal resource for monitoring, research, and education. All GSN data are freely and openly available to the public and scientists around the world from the IRIS Data Management Center." IRIS is funded by NSF GEO/EAR division and IRIS operates part of the GSN (http://www.iris.edu/hq/programs/gsn)

Appendix II

Additional Material for the Record

STATEMENT SUBMITTED BY REPRESENTATIVE JERRY COSTELLO

Mr. Chairman, thank you for holding today's hearing on federally-funded research and development (R&D) threat detection technologies.

After the attacks of September 11th, 2001, early threat detection efforts were increased to counter the growing list of terrorist threats and to prevent a variety of attacks on the U.S. As a result, federal investment in threat detection R&D became a necessary central component of these efforts.

Basic, fundamental science-based research is critical to U.S. strategy for countering terrorism. Already we have seen significant advancements in these technologies that have strengthened our national security and kept America safe. Technologies such as large scale x-ray and gamma ray machines, and airport security technologies such as the Millimeter Wave technology that is helping to detect concealed weapons, explosives, and contraband at our nation's airports.

These are just a few examples of how federal investments in science-based, innovative R&D have direct public benefits and why it is important we provide static funding support to ensure that future technologies reach the maturity necessary to protect against unknown threats.

I am interested to hear from our witnesses regarding how we can ensure the federal government's threat detection efforts anticipate and respond to current and emerging dangers; are pertinent to the Nation's needs; and how the federal government is working with academia and the private sector on these efforts. I also want to know how federal agencies balance and prioritize long-term research activities among ever-changing terrorist threats.

Thank you and I yield back the balance of my time.